A Taxonomy of Attacks on Secure Devices

A J Rae L.P. Wildman

Department of Information Technology and Electrical Engineering,
University of Queensland, Australia.
E-mail: arae @itee.uq.edu.au

Abstract

Evaluating the security of hardware devices requires an organised assessment of which attacks the device might be exposed to. This in turn requires a structured body of knowledge about such attacks, classified in such a way that an evaluator can easily determine which attacks are applicable to a particular device. This paper presents such a collection, organised as a taxonomy of attacks on secure devices. The taxonomy covers many attacks applicable to hardware which are frequently overlooked in a software or protocol-centric evaluation.

Keywords: *Security Evaluation, Taxonomy, Attacks, Secure Devices, Survey, Smartcards, Domain Separation Devices, Hardware Security*

INTRODUCTION

With the spread of pervasive computing, and the increasing publicity given to security breaches in distributed systems, there is a growing need for trusted hardware devices. These devices include stand-alone computers such as personal organisers, hardware implementation of parts of distributed systems, such as ATMs, smartcards and mobile phones, and domain separation devices such as data diodes, filters, data pumps and cryptography modules.

In the context of national security, accepted standards for evaluating hardware devices mandate assessments with respect to vulnerabilities that may be exploited by an attacker (ITSEC 1991, Common Criteria 1999).

Evaluating the security of these devices requires an organised assessment of which attacks the device may be exposed to, and a decision as to whether the device is in fact vulnerable to any of these attacks. This in turn requires a structured body of knowledge about attacks, classified in such a way that an evaluator can easily determine which attacks are applicable to a particular device. Here we do this by reviewing previous classifications of attacks, organising this knowledge into a structured taxonomy, and explaining how it can be used.

CLASSIFICATION OF ATTACKS

Previous Work

Previous attempts to classify attacks have focussed on the techniques used, the resources of the attacker, or the goal of the attack. Our taxonomy below subsumes these existing classifications. For instance, Kommerling et al. (1999) identify four major attack categories:

- **Software Attacks** ‘exploit security vulnerabilities found in the protocols, cryptographic algorithms or their implementation’.
- **Eavesdropping Techniques** ‘monitor the analog characteristics of all supply and interface connections, and any other electromagnetic radiation produced by the processor’.
- **Fault Generation Techniques** ‘use abnormal environmental conditions to generate malfunctions in the processor that provide additional access’.
- **Micro-probing Techniques** ‘access the chip surface directly’.

Abraham et al. (1991), in their analysis of the IBM Transaction Security System, identify three classes of 'adversary' (attacker), and three forms of attack:

- Class I adversaries are labelled as *clever outsiders*. They are intelligent, but lack knowledge about the system, and have access to only moderately sophisticated equipment. Class I adversaries often try to take advantage of existing weaknesses in a system rather than creating new ones.
- Class II adversaries are *knowledgeable insiders*. They are highly educated, and may have detailed understanding of parts of the system. In particular they have potential access to most of the system. Class II adversaries often have access to highly sophisticated tools.
- Class III adversaries are *funded organisations*. They are able to assemble teams (possibly including Class II agents), backed by great funding resources. They are capable of designing sophisticated attacks, and use the most sophisticated tools.

These classes are useful for placing 'reasonableness' bounds on device evaluation. Abraham et al. (1991) argue that the system under evaluation should be secure against Class I and Class II adversaries, but need not be secure from Class III adversaries.

Abraham et al. also put forward a classification based on attack type:

- **Microcircuit attacks** encompass both micro-probing and fault generation. They are equivalent to the `micro-probing techniques' of Kommerling et al. (1999).
- **Counterfeiting attacks** involve an attacker replacing the secure hardware. A successful counterfeit may require a supporting attack to obtain the data necessary for a successful impersonation of the device.
- **Eavesdropping attacks** involve collection of radiated signals. They are equivalent to the Kommerling's eavesdropping attacks.

Howard (2000) introduces the 'STRIDE'categorisation of threats:

- **Spoofing Identity:** Illegally using another user's authentication information.
- **Tampering with Data:** Malicious modification of data.
- **Repudiation:** Plausibly denying having performed an action.
- **Information Disclosure:** Exposing information to individuals who are not supposed to see it.
- **Denial of Service:** Denying service to valid users.
- **Elevation of Privilege:** An unprivileged user gaining privileged access.

Our Taxonomy

Based on this preceding work, we now assemble a structured taxonomy of attacks. In particular, we use the attack categories of Kommerling et al. (1990) as a basis for defining the *access required* by an attacker, and Howard's (2000) threat categorisation to define the *consequences* of an attack.

The basis of our taxonomy is a matrix dimensioned by the *access required* by the attacker, and the *action taken* by the attacker. Within each cell of the matrix, we further differentiate attacks by considering the *consequence* of the attack, and the *method* used for the attack.

In classifying the ***access required***, we consider whether the attacker:

- **possesses** the device – i.e., can open the device and break tamper seals with impunity;
- **handles** the device physically, but cannot break tamper seals on the device;
- **approaches** the proximity of the device, but cannot touch the device; or
- **interfaces** with the device over a network, and can communicate data with the device from either an *insecure* or a *secure domain*.

		Access required			
	ATTACKER	**possesses the device**	**handles the device**	**approaches the device**	**interfaces with the device**
Action	**recover a key**				
	defeat authentication				
	avoid authentication				
	deny service				

Figure 1 Attack Classification Matrix

We recognise that where the fourth category of access applies, an attack on hardware is indistinguishable from an attack on software. Extensive literature already exists on such attacks, including replay attacks, middleman attacks, datatype attacks and passive cryptoanalysis. For examples, see Bieber (1994), Aslam (1996), and Syverson (1994). Therefore, this survey will concentrate on those attacks which are specific to secure hardware; i.e., where the attacker is able to approach or lay hands on the device itself.

In classifying the ***action*** of the attacker, we assume that a legitimate user of the device (or in multi-level systems, a user at a particular access level), is authenticated by a key. This key may be an actual cryptographic key, or may be a password or biometric measure. The attacker thus seeks to:

- **recover a key;**
- **defeat authentication,** for example by setting a key to a known value, or by inducing someone else to supply the key;
- **avoid authentication**, and access data directly; or
- **deny service**, without authentication.

Attacks falling within the same cell of the matrix are differentiated based on the ***consequence*** of the attack, and the ***specific method*** used. Examples of specific methods are described below.

The consequence of the attack may be:

- **modification of data** stored on the device;
- **reading of data** stored on the device;
- **observation of data** transmitted through the device;
- **compromise of cryptography** used by the device; or
- **service denied** to users of the device.

Note that denial of service is both an *action* and a *consequence*. This represents the fact that most attacker goals above are in fact intermediate steps towards some larger aim, whilst denial of service is an end in itself. Note also that where the attacker is able to approach a secure device, denial of service seldom requires more than simply unplugging the device, or attacking it with a hammer. This survey will concentrate on attacks which aim to compromise data or cryptographic protocols.

Having defined the basic elements of our taxonomy, we next show how they are related by putting them in the context of access / goal / method trees.

ATTACKS WITH APPROACH ACCESS

Approach Access is defined as being able to monitor the external characteristics of a device, but not to touch the device itself (Figure 2).

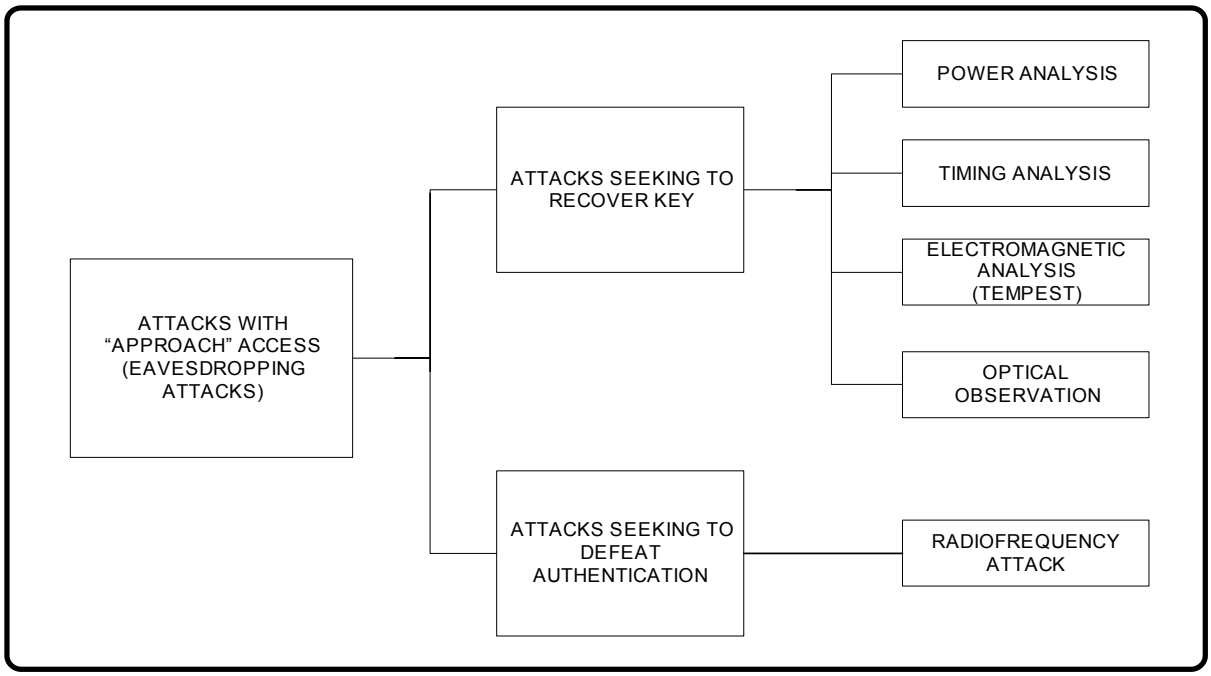

Figure 2 Classification of Attacks with Approach Access

Attacks with Approach Access for the Purpose of Key Recovery

Attacks involving passive observation of external characteristics of a device are termed *eavesdropping attacks*, also sometimes called *side-channel attacks*. The four main observable parameters are power-usage, electromagnetic radiation, device timing, and optical emissions.

Power Analysis

Kocher (1999) discusses two categories of side-channel attack which analyse the power usage of the device. In a *simple power-analysis*, the attacker uses detailed knowledge of the device to identify which instructions are being executed based on their power signatures. In a *differential power-analysis*, the attacker uses a hypothetical model of the device, and refines this model with statistical analysis of the power usage of the device.

Chari et al. (1999) report experimental results demonstrating the feasibility of differential power attacks on smart cards using the 'twofish' algorithm, and discuss the vulnerability of a number of encryption algorithms to power analysis attacks.

Oswald et al. (2003) survey a selection of published side-channel attacks on various algorithms. These include power analysis attacks on modular exponentiation and elliptic-curve cryptosystems. Oswald notes that whilst simple power analysis attacks are often not feasible, differential power analysis attacks are frequently effective, even despite countermeasures.

Electromagnetic Radiation Analysis

A related type of attack monitors the electromagnetic leakage from a device to reconstruct cryptographic material. These attacks are commonly termed *TEMPEST* after the US Military program to counter the problem. Kuhn et al. (1998) surveys the classified and public history of *TEMPEST* research, noting the particular hazards of video displays and radiation leakage across red/black boundaries of multi-level systems.

Rao (2001) reports on practical experiments using electromagnetic monitoring to extract encryption keys from smartcards. These show that the electromagnetic side channel reveals similar information to power analysis, but in the certain cases can leak significantly more information. Anderson (2001) refers to an attack of this nature that can recover card and PIN data from a cash machine at a distance

of eight metres. He also describes a class of attack where a device modulates currents induced by nearby radiofrequency equipment such as mobile phones.

Timing Analysis
The third type of side-channel attack involves the time taken to complete critical operations. Kocher (1996) provides a detailed attack strategy for timing crypto-analysis of several commonly used algorithms. He notes that by measuring the time taken to perform private key operations, attackers can recover the input to those operations, thereby determining the private key.

Optical Observation
Approach access also allows a form of attack where the plain-text key is intercepted before or during input to the encryption module. The most basic such attack is termed *shoulder-surfing* (Loughry 2002), where the attacker observes the user as they input a password or PIN. Loughry (2002) and Kuhn (2002) discuss the feasibility of such attacks, as well as other attacks based on direct observations of optical data, such as reading and decoding LED status indicators.

Attacks with Approach Access for the Purpose of Defeating Authentication

Radiofrequency Attack
Clark (1998) discusses the security of large hardware devices such as ATMs and EFTPOS terminals. He notes that an attacker could use a directional antenna and a radio-frequency generator to produce a large electromagnetic field, forcing the internal random key generators of the device to latch-up and produce predictable keys.

ATTACKS WITH HANDLE ACCESS

Handle Access is defined as being able to manipulate the environment of the device, including setting its inputs and monitoring its outputs (Figure 3). Handle access does not allow opening the device to modify its operation.

Attacks with Handle Access for the Purpose of Key Recovery

Fault Analysis
Anderson et al. (1996, 2001) describe a number of physical attacks on secure devices, intended to cause transient faults in the behaviour of the device. Such attacks include adjusting the input voltage of the device to very high or very low levels, and adjusting the clock frequency of the device. Boneh et al. (1997) discuss how transient hardware faults can be used to break common public key encryption schemes. Biham et al. (1997) discuss a similar technique called *differential fault analysis* for attacking private key encryption devices. These are also termed *Bell-core attacks*. Zheng et al. (1996) describe a technique whereby physical stress is used to cause a pseudo-random number generator to produce predictable output, thereby compromising a private key.

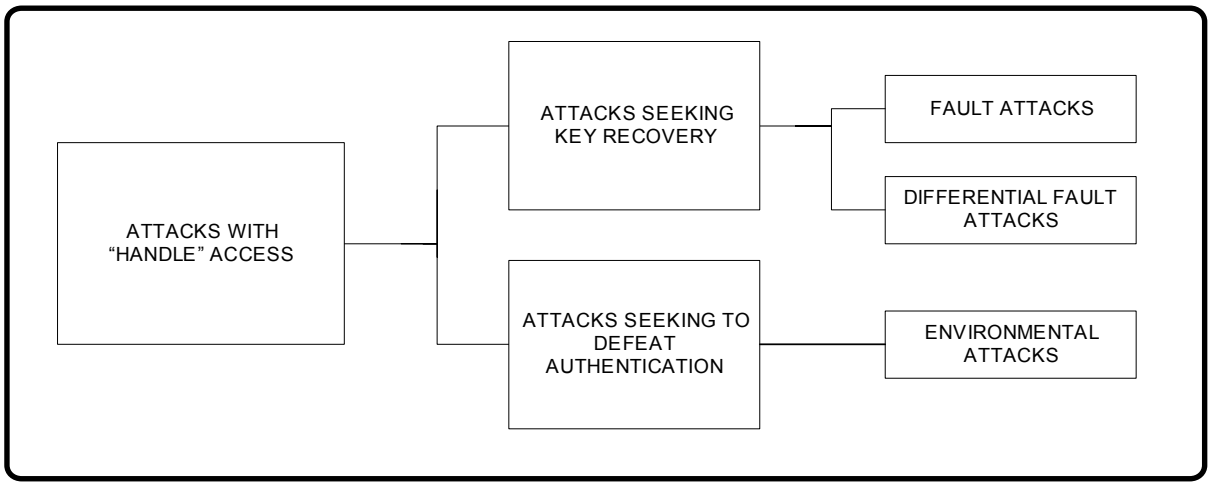

Figure 3 Classification of Attacks with Handle Access

Attacks with Handle Access for the Purpose of Defeating Authentication

Environmental Attacks

Environmental Attacks operate by subjecting the device to extremes of temperature or radiation, typically to erase data stored on the device. Anderson et al. (1996) refer to using ultraviolet radiation to erase EPROMS, thereby restoring phone-cards to their original value. Anecdotes are told of phone-cards which could be recharged by irradiating them in a microwave oven, but there are no credible references for this example.

The consequence of environmental attacks may be to modify data directly, or to defeat authentication by setting a key to a known value.

ATTACKS WITH POSSESSION

Possession, illustrated in Figure 4, is defined as being able to completely manipulate the device, including subjecting the device to sophisticated scanning, or modifying the device. This may be done to devices still in use, or done destructively to learn how a particular class of devices work.

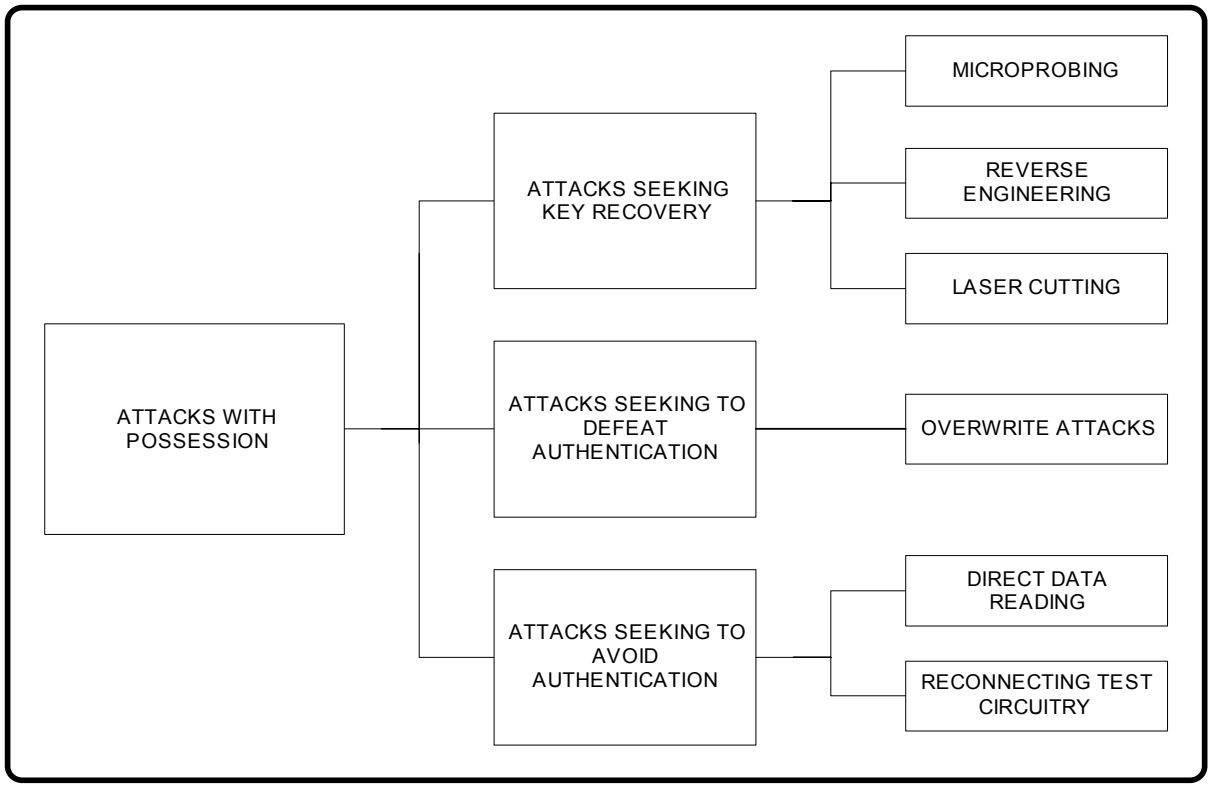

Figure 4 Classification of Attacks with Possession

Attacks Requiring Possession for the Purpose of Key Recovery

Micro-probing

Handschuh et al. (1999) discuss the situation where an attacker can directly read one or more of the execution bits of a device. This is termed a *micro-probing* attack. They show that by observing a few bits of data, an attacker can recover information on the secret key being used by the device.

Kingpin (2000) discusses an attack against the *iKey 1000* USB token device, where the key can be read directly from an exposed part of the circuit.

Huang (2002) reports on an attack using micro-probing to recover the key used to authenticate the Microsoft XBox boot loader.

Reverse Engineering
Some devices are vulnerable to simply removing the data chip from the device, and using nitric acid to remove the protective coating of the chip (Anderson 1996). More professional techniques may involve complete reverse engineering of the device by successively analysing and removing layers of the chip (Blythe 1993).

Further sophisticated techniques include using ultraviolet laser to monitor voltages on the chip (Wiesenfeld 1990), and infrared laser to observe transistor voltages (Ajluni 1995).

Laser Cutting
Anderson et al. (1997) discuss related attacks where laser-cutter microscopes are used to damage the circuit in such a way that the key can eventually be recovered.

Attacks Requiring Possession for the Purpose of Defeating Authentication

Overwrite Attack
An *overwrite attack* replaces the key stored on the hardware with a known value (Anderson 1997)

Kingpin (2000) discusses EEPROM overwrite attacks against the *eToken* and *iKey 1000* USB token devices.

Attacks Requiring Possession for the Purpose of Avoiding Authentication

Reconnecting Test Circuitry
Bovelander (1998) reports on commercial evaluations of smartcards using intrusive techniques. These include probing, scanning electron microscope analysis, and focussed ion beam analysis. A reported example of such an attack is the original version of the *Mondex cashcard*, which was broken by identifying and reconnecting test circuitry (Brown 1997). This attack allowed data on the card to be directly altered.

Glave (1998) reports on Dutch hackers recharging phone cards by directly accessing values stored in EEPROMs.

ATTACKS WITH INTERFACE ACCESS

Interface access attacks focus not on the device itself, but on the protocols that the device uses to communicate with the outside world (Figure 5).

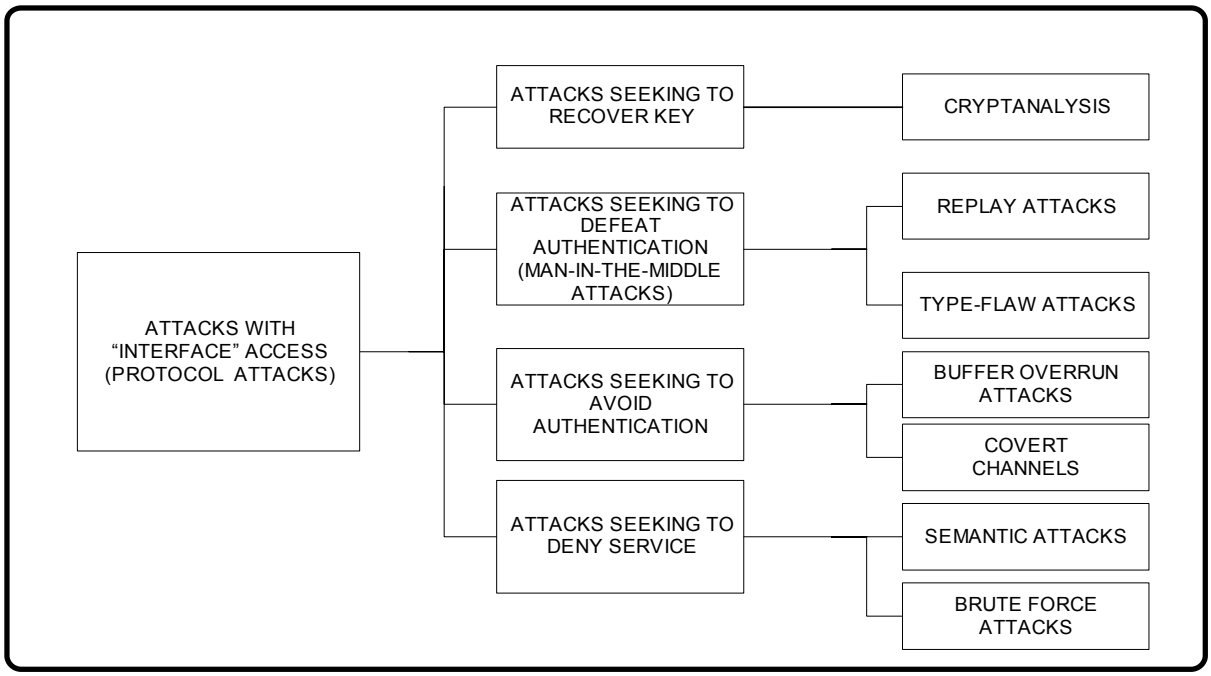

Figure 5 Classification of Attacks with Interface Access

Attacks Requiring Interface Access for the Purpose of Recovering a Key

Cryptanalysis

A *cryptanalysis attack* monitors traffic to and from the device in order to recover the key used to encode that traffic. Brickell et al. (1991) surveys a number of such attacks against various cryptographic schemes. He points out that most of the cryptosystems that had been publicly proposed in the previous decade had been subsequently broken. He claims that the 'one-time pad' is the only cryptosystem known to be unconditionally secure.

Attacks Requiring Interface Access for the Purpose of Defeating Authentication

A *man-in-the-middle attack* intercepts and forges messages in such a way as to induce the device to communicate using a key known to the attacker (Clark et al. 1996).

Replay Attacks

In *replay attacks* (Syverson 1994), the attacker stores messages, and forwards them at unexpected times. One such attack type, a *freshness attack,* involves replay of messages from previous protocol sessions. Another type, *run internal replay attacks*, involve replay of messages from within the same session. A third type, *parallel session replay attacks*, involve replay of messages from a concurrent protocol session.

Type-flaw attacks

In *type-flaw attacks* (Clark et al. 1996) the internal structure of messages is altered in order to induce the device to accept an insecure key, by taking advantage of the ability of certain fields in the message to be interpreted in different ways.

Attacks Requiring Interface Access for the Purpose of Avoiding Authentication

Buffer-overrun attacks

Interface attacks for avoiding authentication are highly implementation specific, as they require mistakes in design or configuration of the device. The broadest class of such attacks are *buffer-overrun attacks* (Aleph One 1996) where the attacker is able to use carefully crafted inputs to cause insecure operation of the device.

Covert Channels

A *covert channel* is a mechanism via which information may be deliberately communicated between parts of a system at different security levels. We distinguish between *eavesdropping* attacks, where the attacker has proximity access to the device but no interface access to the device, and *covert channels* where the attacker can manipulate data within the secure domain of the system.

Note that passive side-channels such as power and radiation can be converted into covert channels by prompting device behaviours which exaggerate the observable characteristics of the device.

Covert channels are classified as *storage channels*, *timed channels*, and *mixed channels* (Moskowitz 1994).

A storage channel is one where the unclassified part of the system (called 'Low') receives different signals in response to its actions depending on the state of the classified system ('High'). For example, a High process might adjust the access permissions of a file as a means of conveying a message to a Low process, which can see the permissions but not read the file.

A timing channel is one where a Low process receives the same signals, but with different response times depending on the behaviour of a High process. A mixed channel is where a Low process receives different signals with different response times.

Attacks Requiring Interface Access for the Purpose of Denial of Service

Semantic and brute force attacks

Denial of service attacks using the interface are either *semantic attacks* or *brute force attacks* (Mirkovic 2002). A *semantic attack* sends incorrectly formed packets or messages to the device in order to consume resources. A *brute force attack* sends large numbers of correctly formed messages.

USE OF THE TAXONOMY

Now that we have established the taxonomy, we take a brief look at its application.

Classification and Understanding of Attacks

To ensure that a device is secure against malicious interference, we need to analyse and understand the ways in which the device can be attacked. The taxonomy thus facilitates understanding by categorising and grouping attacks that share similar characteristics.

The taxonomy also serves as a realistic overview of the challenge that faces designers of secure devices. It is important that a design has mechanisms to defend against the entire spectrum of attacks which may be used against it.

Determining an Attack Profile for Evaluation

The matrix of Figure 1 can be used to determine the threats extant for a particular device. These threats form an attack profile which serves as a checklist against which the device may be evaluated. Note that the attack profile for a device may change across the device's lifecycle. A device may be attacked during manufacture or distribution, by its owner, by third parties during use, or after disposal.

A column of the matrix can be eliminated if the planned usage of the device prevents an attacker from gaining that form of access.

For example, for an automatic teller machine, it might be assumed that a customer will not have *handle* or *possess* access to the machine's internals, whereas a technician might have *handle* but not *possess* access. For a smart card, the holder of the card has complete access, whereas a card reader has only *interface*, *approach* and *handle* access.

Rows of the matrix may also be eliminated. For example, if data is not protected by cryptography, then the rows corresponding to *recover key* and *defeat authentication* can be removed. Alternately, denial of service may not be a threat for some devices, so long as the data remains secure.

All of the remaining cells in the table are potential threats against which the device must be examined for vulnerability. The attack methods relevant to each cell in the table can be derived from the trees in Figures 2 to 5. Individual attacks may be eliminated from the profile if they do not serve an attack goal relevant for the particular device, or if the resources required are too expensive for any perceived threat.

For example, Figure 6 shows the attack profile for a cryptographic device. The operating environment for this device ensures that an attacker cannot *possess* the device. Further, it has been determined that denial of service is not a threat for this particular application of the device.

		Access Required		
	ATTACKER	**handles the device**	**approaches the device**	**interfaces with the device**
Goal	**recover a key**	Fault attacks, Differential fault attacks	Power analysis, Timing analysis, EMR analysis Optical analysis	Passive cryptanalysis
	defeat authentication	Environmental attacks	Radiofrequency Attack	Replay attacks Type-flaw attacks
	avoid authentication	Timed channels, Storage Channels, Mixed Channels		Buffer-overrun attacks

Figure 6 Example Attack Profile for a Cryptographic Device

Note that this matrix focuses attention on those attacks which are relevant to the device in this particular mode of operation.

Improving Security Technology

Krsul (1997) argues:

Virtually every field where failure can be catastrophic has recognised that accumulation of information about failures is critical to the stepwise refinement of technology, particularly when the systems that fail are highly complex.

This is particularly true in the security field, where institutional reluctance to reveal information about attacks, failures and vulnerabilities has thinned the public knowledge of realistic attack information (Anderson 1994). As a result, most of the literature on attacks focuses on protocol vulnerabilities (Syverson 1994, Rice 2000), with little information about whether these attacks pose practical threats to real devices.

By classifying and organising information about attacks, and linking theoretical attack methods with reports of experiments and actual vulnerabilities, it is hoped that the above taxonomy will aid in the identification of new attacks, and in the development of techniques for addressing existing and future attacks.

ACKNOWLEDGEMENTS

This research was funded by Australian Research Council Linkage Grant LP0347620, '*Formally-Based Security Evaluation Procedures*'.

REFERENCES

Abraham D.G., Dolan G.M., Double G.P., and Stevens J.V. (1991) *Transaction security system*. IBM Systems Journal, 30(2):206–228.

Ajluni C. (1995) *Two new imaging techniques promise to improve IC defect identification*. Electronic Design, 43(14):37–38, July.

Aleph One (1996) *Smashing the stack for fun and profit*, Phrack 49

Anderson R. (1996) *Why cryptosystems fail*. In Practical Cryptography for Data Internetworks, IEEE.

Anderson R. (2001) *Security Engineering for Distributed Systems.* Wiley.

Anderson R. and Kuhn M. (1996) *Tamper Resistance – a Cautionary Note*. In Proceedings of the Second Usenix Workshop on Electronic Commerce, pages 1–11, November.

Anderson R. and Kuhn M. (1997) *Low cost attacks on tamper resistant devices*. In Lecture Notes in Computer Science 1361, pages 135–136. Springer-Verlag.

Aslam T., Krsul I., and Spafford E. H. (1996) *Use of a taxonomy of security faults*. In Proc. 19th NIST-NCSC National Information Systems Security Conference, pages 551–560.

Bieber P. and Boulahia-Cuppens N. (1994) *Formal development of authentication protocols*. In D. Till, editor, Sixth Refinement Workshop, pages 801–802. Springer-Verlag.

Biham E, and Shamir A. (1997) *Differential fault analysis of secret key cryptosystems*. Lecture Notes in Computer Science, 1294, Springer-Verlag.

Blythe S., Fraboni B., Lall S., Ahmed H., and de Riu E. (1993) *Layout reconstruction of complex silicon chips*. IEEE Journal of Solid-State Circuits, 28(2):138–145, Feb.

Boneh D, DeMillo R.A., and Lipton R.J. (1997) *On the importance of checking cryptographic protocols for faults.* Lecture Notes in Computer Science, 1233:37–51, Springer-Verlag.

Bovelander (1998) *Smart card security - How can we be so sure?* In Lecture Notes in Computer Science, number 1528, pages 332–337. Springer-Verlag.

Brickell E.F. and Odlyzko A.M. (1991) *Cryptanalysis: A survey of recent results*. In G. J. Simmons, editor, Contemporary Cryptology, pages 501–540. IEEE Press.

Brown, R. (1997) *Leaked national bank memo confirms pilot of Mondex broken*. Computerworld News Wire, September.

Chari S., Jutla C., Rao J.R., and Rohatgi P. (1999) *A cautionary note regarding evaluation of AES candidates on smartcards*. In Second Advanced Encryption Standard (AES) Candidate Conference, Rome. http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm.

Clark A.J. (1988) *Physical protection of cryptographic devices*. In D. Chaum and W.L. Price, editors, Lecture Notes in Computer Science 304, pages 83–93. Springer-Verlag.

Clark J. and Jacob J. (1996) *Attacking Authentication Protocols*. High Integrity Systems 1(5):465–474

Common Criteria (1999) *Common Criteria for Information Technology Security Evaluation. Part 2: Evaluation Methodology*. http://www.commoncriteria.org.

Glave J. (1998) *Pirates cash in on weak chips*. http://www.securityfocus.com/elsewhere/1998/5.

Handschuh H., Paillier P., and Stern J. (1999) *Probing attacks on tamper-resistant devices*. In Cryptographic Hardware and Embedded Systems, pages 303–315.

Howard M. (2000) *Secure systems begin with knowing your threats.* http://archive.devx.com/upload/free/Features/zones/security/articles/2000/10oct00/mh1000[1]-1.asp

Huang J. (2002) *Keeping secrets in hardware: The Microsoft Xbox case study*. Technical report 2002-008, Massachusetts Institute of Technology - Artificial Intelligence Laboratory.

ITSEC (1991) *Information Technology Security Evaluation Criteria*. Department of Trade and Industry, London.

Kingpin (2000) *Attacks on and countermeasures for USB hardware token devices*. In Proceedings of the Fifth Nordic Workshop on Secure IT Systems Encouraging Co-operation, pages 35–57. Reykjavik University.

Kocher P. (1996) *Timing attacks on implementations of Diffe-Hellman, RSA, DSS, and other systems*. Lecture Notes in Computer Science, 1109:104–113, Springer-Verlag.

Kocher P., Jaffe J., and Jun B. (1999) *Differential power analysis*. Lecture Notes in Computer Science, 1666:388–397, Springer-Verlag.

Kommerling O. and Kuhn M.G. (1999) *Design principles for tamper-resistant smartcard processors*. In Proceedings of the USENIX Workshop on Smartcard Technology, pages 9–20. Chicago, 10–11 May.

Krsul I., Spafford E., and Tripunitara M. (1998). *Computer vulnerability analysis*. Technical report TR98–07, COAST Laboratory, Purdue University, May.

Kuhn M.G. (2002) *Optical time-domain eavesdropping risks of CRT displays.* In Proceedings of the 2002 IEEE Symposium on Security and Privacy, pages 3–18.

Kuhn M.G. and Anderson R.J. (1998) *Soft Tempest: Hidden data transmission using electromagnetic emanations*. Lecture Notes in Computer Science, 1525:124–142, Springer-Verlag.

Loughry J. and Umphress D.A. (2002) *Information leakage from optical emanations*. ACM Transactions on Information and Systems Security, 5(3):262–289.

Mirkovic J. and Reiher, P. (2002) *A Taxonomy of DDoS Attack and DDoS Defence Mechanisms*, University of California Technical Report #020018.

Moskowitz I.S. and Kang M.H. (1994) *Covert channels - here to stay?* In Compass '94, pages 235–243. IEEE Press.

Oswald E. and Preneel B. (2003) *A survey on passive side-channel attacks and their countermeasures for the Nessie public-key cryptosystems*. Technical Report NES/DOC/KUL/WP5/027/1. http://www.cosic.esat.kuleuven.ac.be/nessie/reports/.

Rao J.R. and Rohatgi P. (2001) *EMpowering side-channel attacks*. Cryptography ePrint Archive 2001/037. http://eprint.iacr.org/2001/037/.

Rice G. and Davis J. (2000) *A genealogical approach to analyzing post-mortem denial of service attacks*. Secure and Dependable System Forensics Workshop, University of Idaho, September 23-25, 2002

Syverson P. (1994) *A taxonomy of replay attacks*. In Computer Security Foundations Workshop VII. IEEE Computer Society Press.

Wiesenfeld J.M. (1990) *Electro-optic sampling of high-speed devices and integrated circuits.* IBM Journal of Research and Development, 34(2/3):141–161, March/May.

Zheng Y. and Matsumoto T. (1996) *Breaking smart card implementations of ElGamal signature and its variants*. Presented at the rump session of Asiacrypt'96. http://www.pscit.monash.edu.au/~yuliang/