Security Research at Cambridge

Ross Anderson

October 30 2012

The New Grand Challenge

- Global-scale socio-technical systems are growing more complex as computers and communications are embedded everywhere
- How are we to understand them, manage them and improve them?
- How do we make them dependable in the face of malice, error and mischance?

Roman Army

October 30 2012

Bank of England

October 30 2012

What happens when you add software?

October 30 2012

What happens when you add software?

- “You know you’ve got a distributed system when you can’t get your work done because of the failure of a computer you’re never heard of”
  - Leslie Lamport

Phish sent to Dalai Lama's office

Subject: Kalon Tripa Succession
From: "Pema Rinzin" <prinzintibet@yahoo.com>
Date: Thu, September 18, 2008 8:14 am
To: choejor@dalailama.com

Dear Sir,

Attached please find the final Tibetan translation of my English announcement for the Kalon Tripa succession initiative. Response to my press release on September 2nd has been very positive and I have been receiving lots of email and phone messages from Tibetans everywhere.

I am trying to get someone to translate the Kalon Tripa Hochoe into English, but if you already have it translated, please send it to me.

Any advice from you in this initiative of mine would be greatly appreciated.

Yours sincerely,

Pema Rinzin
President
TAC

Official Photographer/webmaster
Office of His Holiness the Dalai Lama
Thekchen Choeling
P/O Mcleod ganj 176219
Dharamsala (H.P.)
India

Oc

British Crime Survey

- Asks 44,000 people whether they've been a victim of crime each year
- Acquisitive crime in 2009–10: about 1 million traditional 'serious' crime (burglaries, thefts of and from vehicles …)
- About 2–3 million other (dodgy auctions, credit card disputes, online banking …)
- So in volume terms at least, cyber crime is now most of it

Terminal tampering

- Banks said terminals were hard to tap
- But they lied …
- Bugs installed in a warehouse in Dubai, card and PIN data texted to Karachi
- Police dropped charges when banks wouldn't help prosecute

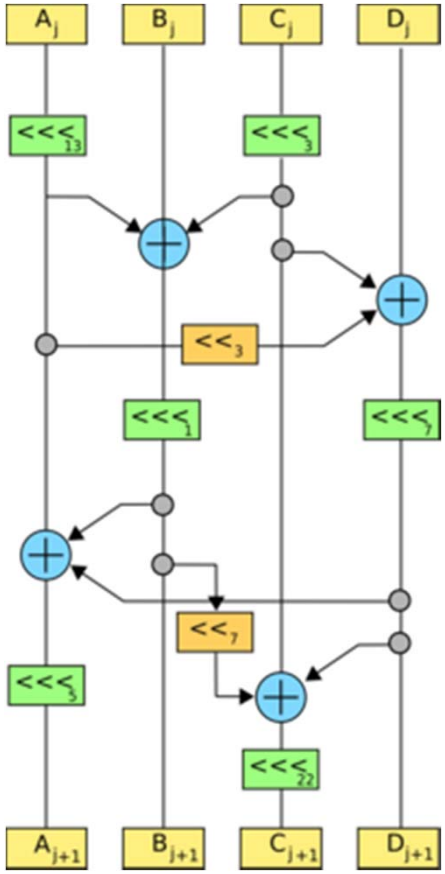
The ‘No PIN’ attack

- How could crooks use a stolen card without knowing the pin?
- We found we could insert a device between card & terminal
- Card thinks: signature; terminal thinks: pin
- On Newsnight on Feb 2010 – still not fixed!

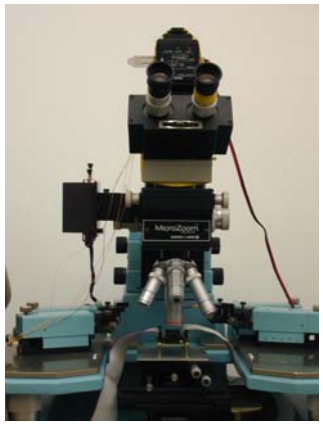
Security Engineering

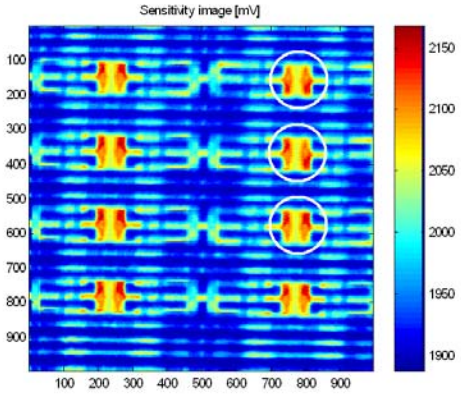
- Medicine = chemistry + physiology + psychology + … ?
- Architecture = civil engineering + art history + project management + … ?
- …
- Security engineering = ?

Mathematics …



… and metal





- Semi-invasive attacks
- Light ionises silicon, causing leakage current
- Can read out memory contents directly –o r change them!
- Now: combo attacks (lasers plus power analysis)

… and protocols

- Distributed system to thwart censorship
- Inspired gnutella, freenet, … peer-to-peer movement
- Now extending to analysis of APIs

… and operating systems

- CHERI – a MIPS device with capabilities
- Fine-grained mandatory access controls

… and economics

- Since 2000, we have started to apply economic analysis to IT security and dependability
- It often explains failure better!
- Electronic banking: UK banks were less liable for fraud than US banks, so got lazy and careless: ended up suffering more internal fraud and more errors
- AV software less effective: ten years ago, AV software recognised >90% of new malware, but now you're lucky to spot 30%
- Why is Microsoft software so insecure, despite market dominance?

… and psychology

- Phishing only started in 2004, but in 2006 it cost the UK £35m and the USA perhaps $200m
- Banks react to phishing by ‘blame and train’ efforts towards customers (which we know doesn’t work from the safety-critical world)
- We really need to know a lot more about the interaction between security and psychology
- What’s the best way to deter deception online?

Emerging topics

- Next-generation operating system security
- What next after BGP SEC: SDN SEC
- Next-generation mobile device security
- Hardware: attacking ever-smaller devices
- Malware reverse engineering and analysis
- Systems: radical alternatives to passwords
- Econometrics of cyber-crime
- Psychology: deterrence of deception
- What else?