

The Internet: A Secure Platform for e-Commerce?

Paul C. Van Oorschot

Digital Security Group
Carleton University, Ottawa, Canada

May 16, 2005

“Identity-theft case costs taxpayers \$540,400”

The Globe and Mail, April 12 2004

- 89-year-old owns a \$1 million Calgary property
- “buyer”, “seller” meet lawyer (false driver’s license, SIN)
- property transfer is registered
- \$500K mortgage
- money moves through several accounts . . .

What is Identity Theft?

- exploitation of another's identity-corroborating info

Allows criminal activities, e.g.:

- obtain fraudulent ID credentials, CC's, loans
- open new bank accounts in stolen name
- take over existing accounts

Identity Theft – Why So Easy?

Fundamental underlying problems:

1. ease of duplicating personal data and credentials;
2. difficulty of detecting a copy of a credential; and
3. when credential info is used by an impersonator to obtain new credentials, no immediate notice to original owner

Online Identity Theft – Even Easier

Online ID theft is further facilitated by:

- lower risk to attacker (not physically present - anonymity)
- large-scale attacks much easier
- availability of personal information on the Internet (e.g. full credentials stored at servers)
- poor custodianship –examples from 2005:
 - ChoicePoint: 145,000 consumer records bought
 - B of A: 1.2million records, stolen backup tapes
 - break-ins to server databases

From: CITIBANK [mailto:antifraud.ref.num12571006617289@citibank.com]

Sent: October 4, 2004 11:07 AM

Subject: CitiBank - Client's Data Verification [Mon, 04 Oct 2004 12:05:09]

Dear CitiBank Customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details. This process is mandatory, and if not completed within the near time your account may be subject to temporary suspension. To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_steup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi(R) Identity Theft Solutions

CitiCorp

Do not reply to this email as it is an unmonitored alias.

A member of citigroup
Copyright (C) 2004

Phishing and Key Logging

phishing kits now available on the Internet

- to create bogus websites, and use spamming software

key logging – e.g. trojan Bankhook.A

- spreads by browsing (June 29 2004)
- exploits IE vulnerability
- on detecting connect attempts to any of 50 online banks, records sensitive info pre-SSL, mails to remote computer

Passwords

- user interface / convenience vs. security
- too many, poorly chosen, reused
- the logic of changing passwords
- security in light of phishing and key-loggers
- Moore's law and exhaustive search
- distinguishing computers from humans

Computer Worms

- Slammer (Jan. 2003): single-packet UDP worm
 - 90% of vulnerable hosts infected in 10 min
 - scanning rate: 55M scans/sec after 3 minutes
 - payload: non-malicious
- hit-lists and flash worms (10's of seconds)
- mass-mailing worms; IM

Anti-Virus Software

- AV-engine vs. signature updates
- free but still not universally used
- curiosity

Firewalls

- the Internet is about being connected
- Swiss cheese
- tunneling over port 80 (or SSL)

Intrusion Detection Systems (IDS)

- misuse-based, anomaly-based
- volume of logs - skilled personnel to monitor
- false positives
- false negatives; zero-day incidents
- attack speed vs. limits of human intervention
- “Houston, we have a problem”

“Just Use Stronger Crypto”

- “we need stronger crypto”
 - stronger door locks; windows wide open
- security vs. cryptography – consider malware
- Internet threat model & SSL vs. hostile host model

Public Key Infrastructure (PKI)

- key management: still the real challenge in practice
 - difficult to get right, difficult to deploy
- “blind man does business with stranger in foreign land”
- “if only there were a global PKI”
 - communities of trust

Formal Analysis and Provable Security

- “proofs” of security vs. reality
- assumptions and models
- tools promoting “useful thinking” remain valuable
- trial and error; experience and soak-time

Botnets – Ultimate Weapon?

- IRC: 1-to-many real-time communication
- botnet: compromised PCs managed from an IRC channel
- typical size: 2-10,000; 50,000+ observed (100,000's)
 - going rate for SPAM proxying: 3-10cents/host/week
- 1000 PC's, average upstream 128KBit/s = 100MBit/s+
- DDoS, spam, bootstrapping malware spread, phishing

Software: Second-Weakest Link

- brick houses on quicksand
 - price of software; pace of change
- monoculture vs. diversity
- buffer overflows and related vulnerabilities
 - progress since 1988 Morris worm?

The Weakest Link: Users and UI

- false security of passwords
- systems more complex, users more inexperienced
 - no time, no interest, no ability to learn
- astounding lack of human factors design, and research
- no way to trust browser interfaces (what site are you at?)

Other Internet Trends

- vendors regularly ship software with known vulnerabilities
 - compare to automobiles
- more malicious activity for \$ gain = organized crime
- wireless
- IP convergence (e.g. VoIP)

What is Needed?

- stronger authentication for accountability, traceability
- stronger laws, penalties for bad software / practices
 - but be careful (DMCA problem; jurisdictional issues)
- security issues to cause big software vendors more pain
 - civil liability? higher insurance costs?

Concluding Remarks

- tremendous lack of computer / network security expertise
- boundless open problems in Internet security
- Risk = Threat x Vulnerability x Asset_Value
 - difficult to measure “Threat”
 - is “Risk” acceptable for e-commerce?

Thank you



Paul C. Van Oorschot

Canada Research Chair in Network & Software Security

Carleton University – School of Computer Science

Spam

- spoofed From addresses
- Owned machines; open proxies
- SPF (sender policy framework); DomainKeys
- legitimate domains bought, used, abandoned