Hacking Trust

Security may seem but cannot be.


"Truth may seem, but cannot be:
Beauty brag, but 'tis not she;
Truth and beauty buried be.”

Anthony C. Zboralski
z@bellua.com

Dave McKay
d@bellua.com
Hacking Trust; 
Security may seem but cannot be

• Introduction
  • Anthony Zboralski <z@bellua.com>
  • Dave McKay <d@bellua.com>

• What is Trust?
  • 1. firm belief in the reliability, truth, ability, or strength of someone or something 2. acceptance of the truth of a statement without evidence or investigation

• What is a Network of Trust?
  • A network of trust consists of anything which interacts directly or indirectly with our target.
  • A good example is sharing a secret.
Real Life Network of Trust
Case Study: Software

- Compilers, Interpreters, IDS/IPS, Sendmail, SSH, FTP, E-Mail Clients, Databases, Instant Messengers, Games...

- Core Banking System; the accounts don’t balance when the bank restricts vendor access

- Daylite and OpenBase remote authentication by-pass (0day)


“Enhanced Security: OpenBase SQL has undergone a security audit that has lead to improvements security in OpenBase 9.0.”
SQL Injection ->
-login "' or 1=1;"
password is ignored
and default user, admin
is used.
A lame security hole in the underlying database give us access to daylite username and passwords ->

Daylite
Clear-text Passwords ->
Case Study: Financial Consultants

• **Stockbrokers**
  - Ivan Boesky, Michael Milken
  - Your Personal Broker

• **Accountants & CFO**
  - Enron
  - Worldcom

• **Mergers and Acquisition**
  - Who do you hack?
    - The Bankers
    - The Lawyers
Case Study: Telcos

• “End to End” Frame-relay Links

• VSAT Networks
  • Why many banks all over Asia use VSAT connections in clear-text?
  • Substantial drop in performance when using IPSEC as it breaks some of transport flow optimization (TFO) features.

• The Effect of Convergence
  • GSM, SMS
  • SMS Banking
  • Value Added Services Partners

• Trusting the Backbone.
  • Wireless backup link of a Bank
Captured ATM Transactions over Wireless

CENSORED

You should have joined HITBSecConf 2006... If you really wanted to see this slide.
One year later, similar bank - similar problems...

CENSORED

You should have joined HITBSecConf 2006... If you really wanted to see this slide.
Do it Yourself: Reset and Approve your Credit Card Limit

CENSORED

You should have joined HITBSecConf 2006... If you really wanted to see this slide.
Case Study: Government Intelligence

- Soviet Union
  - December 25th, 1991

- China
  - Reverse Engineering
  - LANL

- NSA & FBI
  - Echelon
  - Carnivore
Case Study: Internet Service Provider

• Hijacking the domain name of an Online Banking ASP

• Hacking the ISP to steal e-mails of a target using tunnelx
  • 1st occurrence: ISP replaced the target’s cisco router
  • 2nd occurrence: ISP hides the real target

• MPLS
  • a “cost-effective” way to provide access, intranet and extranet VPN services.

• Hotel ISP (live demo)
Case Study: Employees

• Corporate
  • Workers
  • Custodians

• Government
  • Background Checks

• Household
  • Maids
  • Au Pair and Babysitters

• Hackers
  • Consultants or Sociopaths?
Conclusion

• Current largest threat remains your network of trust.

• Who killed Julius Caesar?
  • Betrayal always comes from the people you trust

• Your network of trust MUST BE included within the scope of your compliance check and regular security assessment

• Trust and Mistrust is a vicious circle
Q&A

- Any Questions?