

# Current Threats & Countermeasures

ACCUVANT



Jon Miller CISSP  
Director of Services – Security Evangelist  
jmiller@accuvant.com



“Oh hey! I just love these things! ... Crunchy on the outside and a chewy center!”

ACCUVANT



# Agenda

---

- The Changing Landscape of Security Architectures
- Modern Attack Vectors
  - Attack Frameworks
  - Wireless Networks
    - Bypassing Security Controls
  - Web Applications
  - Physical Security
    - Lockpicking for the lazy/efficient
  - RFID Hacking
- Solutions and Mitigation Strategies

# Identity Theft

---

[www.idtheftcenter.org](http://www.idtheftcenter.org)

**In 2007, ITRC documented 446 paper and electronic breaches, potentially affecting more than 127 million records.**

**This is a significant increase from 2006 which listed in excess of 315 publicized breaches affecting nearly 20 million individuals.**

**In 2005 there were 158 incidents affecting more than 64.8 million people.**

**Based on ITRC's categorization, the 2007 breaches break down as follows:**

**24.5% government/military agencies**

**24.7% from educational institutions**

**29.3% from general businesses**

**14.5% from health care facilities / companies**

**7% from banking / credit / financial services entities**

# What is a BREACH?

---

The following criteria have been used by the Identity Theft Resource Center in the formulation and development of its breach list.

**Criteria for personal identifying information: Any name or number that may be used, alone or in conjunction with other information, to identify a specific individual including:**

**Name, Social Security number, date of birth.**

**Banking or financial account number, credit card or debit card number with or without PIN, official State or government issued driver's license or identification number, passport identification number, alien registration number, employer or taxpayer identification number, or insurance policy or subscriber numbers**

**Unique biometric data**

**Electronic identification number, address or routing code or telecommunication identifying information or device**

The list does NOT include occurrences when just a name, phone number and address (home or email) are exposed.

A breach may be the loss or theft of paper or electronic data

# Jan 08 to Present / Public Breaches

---

## Banking –

- Compass Bank – 1,000,000 records
- Target National Bank – UNKNOWN
- Davidson Companies – 226,000 records
- IronMountain / GE – 650,000 records

## Businesses –

- Agilent – 51,000 records
- Hannaford Bros Supermarket – 4,200,000 records
- MTV – 5,000 records
- Kraft Foods – 20,000 records
- Salesforce.com – UNKNOWN
- Horizon BC/BS – 300,000 records
- Google – UNKNOWN

## Education –

- Harvard University – 6,600 records

# 8,391,871 Records Exposed 1/08-4/08

---

## **Banking/Credit/Financial (22.4% Identified Records)**

**Reported Breaches – 12**

**Records Exposed – 1,879,619**

## **Business (64.9% Identified Records)**

**Reported Breaches – 60**

**Records Exposed – 5,444,422**

## **Educational (2.9% Identified Records)**

**Reported Breaches – 42**

**Records Exposed – 240,076**

## **Government Military (4.8% Identified Records)**

**Reported Breaches – 30**

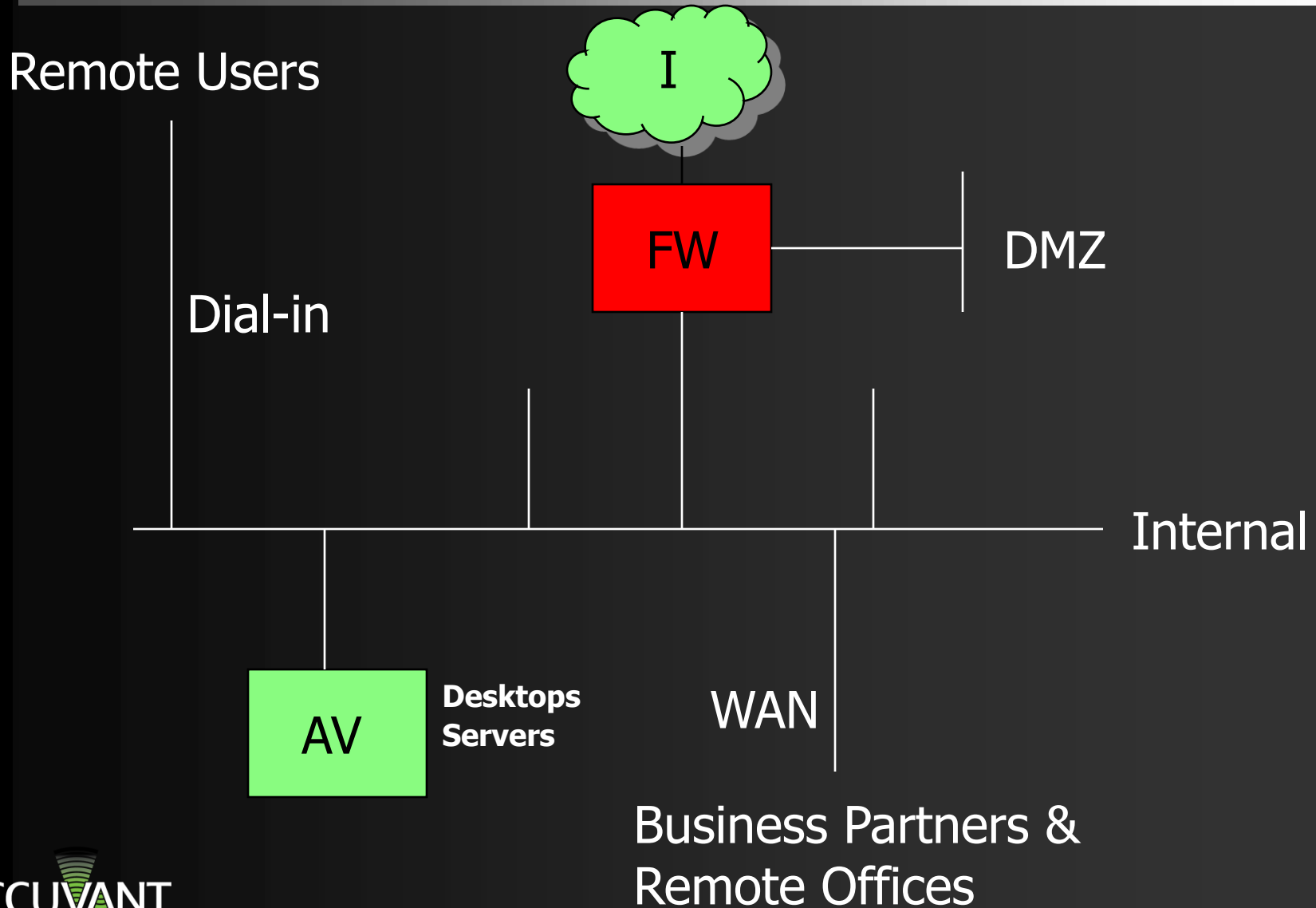
**Records Exposed – 400,424**

## **Medical Healthcare (5.1% Identified Records)**

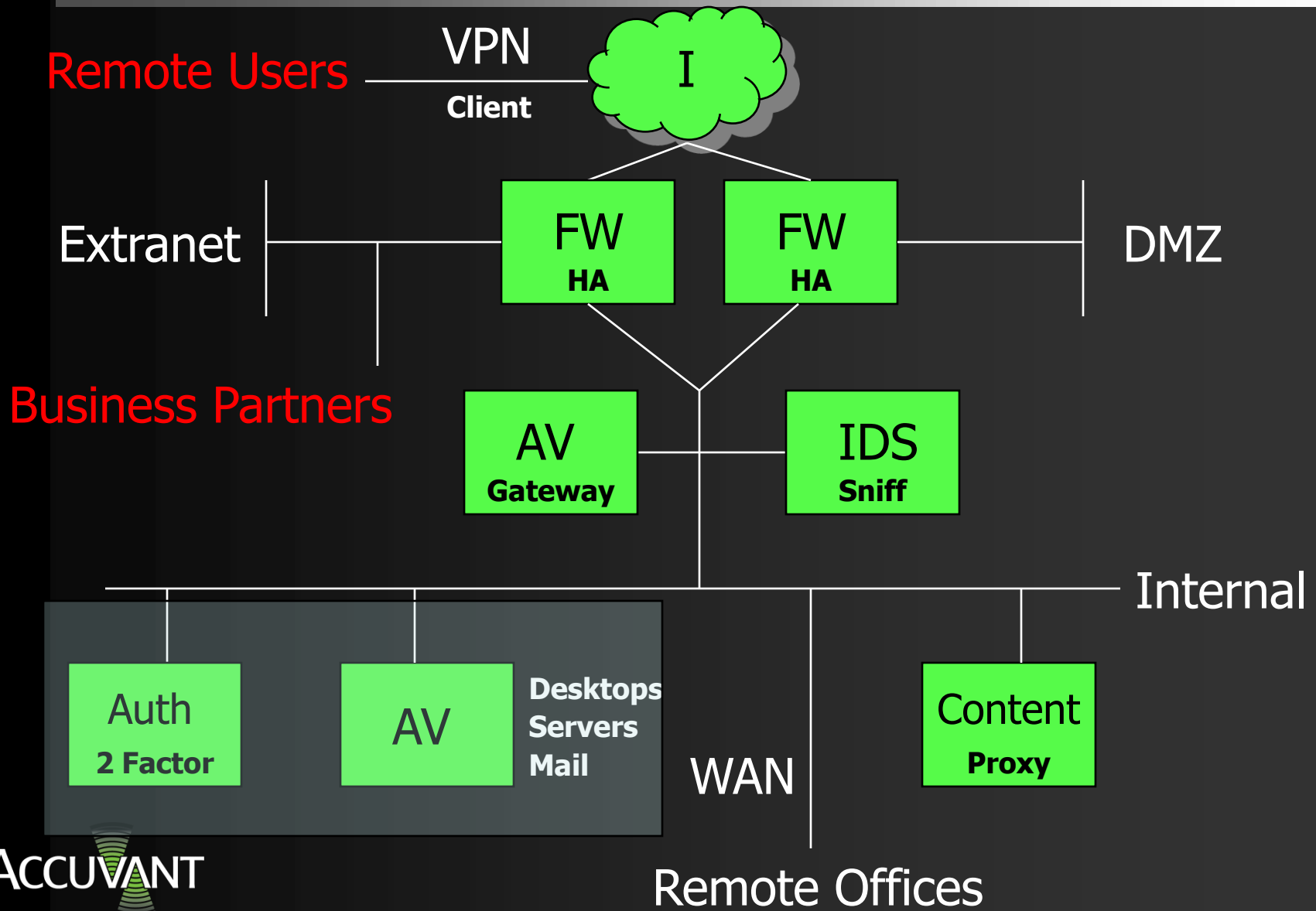
**Reported Breaches – 23**

**Records Exposed – 427,330**

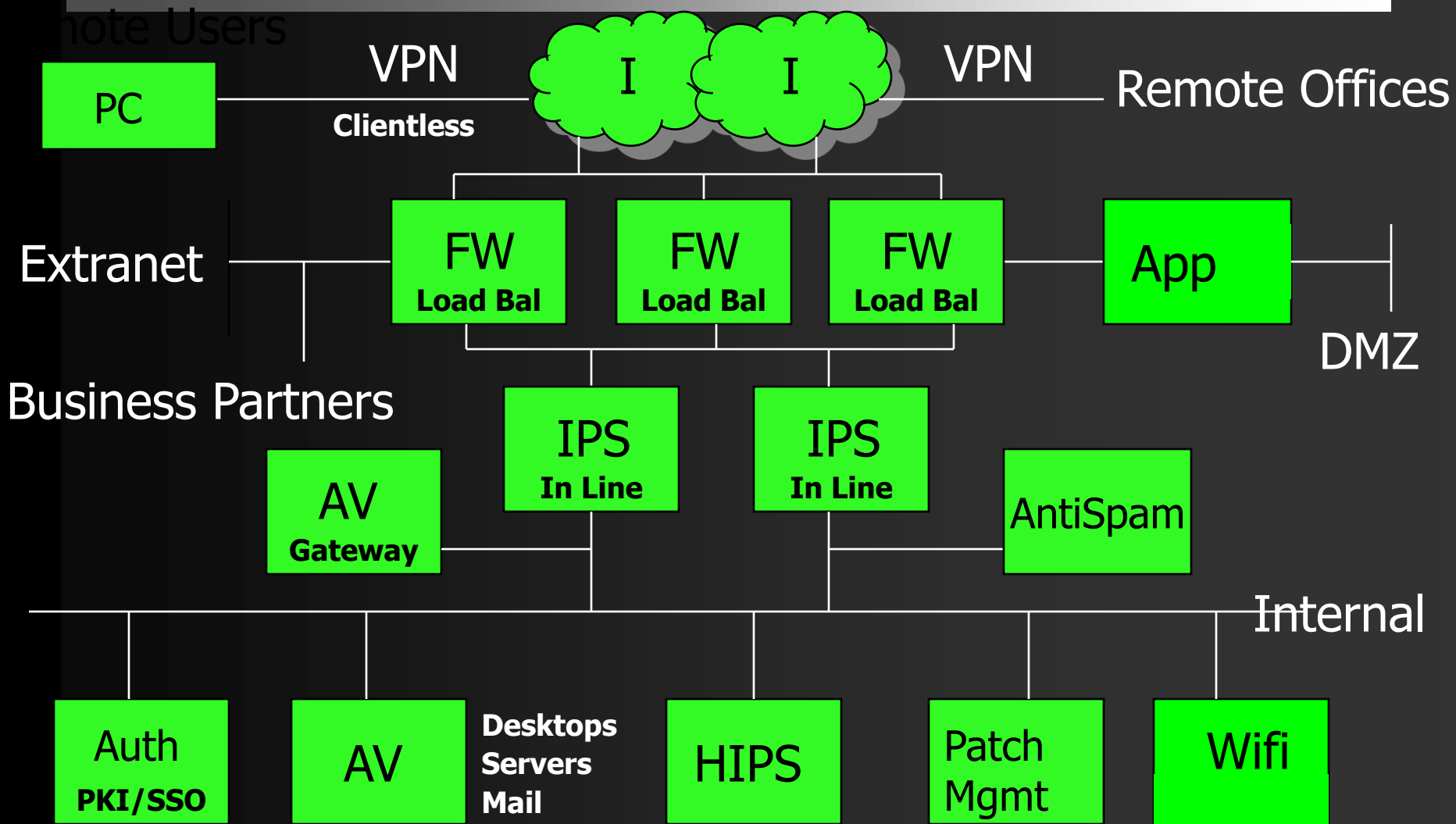
# Security Architecture - 1999



# Security Architecture - 2001



# Security Architecture - 2008



---

As Architectures Have Changed,  
So Have the Hackers Techniques

# Traditional Exploits Tools & Techniques

---

- Public Code / Reverse engineering
  - Patch Tuesday = Exploit Wednesday
- Exploit Frameworks
  - MetaSploit
  - Canvas (Immunity Security)
  - Mosquito
  - IMPACT (CORE technologies)

# Traditional Exploits— Exploit Frameworks



- 3Com 3CDAemon FTP Server Overflow
- AOL Instant Messenger goaway Overflow
- \* AWStats configdir Remote Command Execution
- Alt-N WebAdmin USER Buffer Overflow
- Apache Win32 Chunked Encoding
- AppleFileServer LoginExt PathName Overflow
- \* Arkeia Backup Client Remote Access
- Arkeia Backup Client Type 77 Overflow (Mac OS X)
- Arkeia Backup Client Type 77 Overflow (Win32)

```

globalscapertp_user_input  GlobalSCAPE Secure FTP Server user input ove
ow
gnu_mailutils_imap4d       GNU Mailutils imap4d Format String Vulnerab
y
hpux_ftpd_preauth_list    HP-UX FTP Server Preauthentication Directory
string
hpux_lpd_exec              HP-UX LPD Command Execution
ia_webmail                 IA WebMail 3.x Buffer Overflow
icecast_header            Icecast (<= 2.0.1) Header Overwrite (win32)
ie_objecttype             Internet Explorer Object Type Overflow
iis40_htcr                 IIS 4.0 .HTB Buffer Overflow
iis50_printer_overflow    IIS 5.0 Printer Buffer Overflow
iis50_webdav_ntdll        IIS 5.0 WebDAV ntdll.dll Overflow
iis_fp30reg_chunked       IIS FrontPage fp30reg.dll Chunked Overflow
iis_nsislog_post          IIS nsislog.dll ISAPI POST Overflow
iis_source_dumper         IIS Web Application Source Code Disclosure
iis_v3who_overflow        IIS v3who.dll ISAPI Overflow
imail_imap_delete         IMail IMAP4D Delete Overflow
imail_lmtp                 IMail LMTP Service Buffer Overflow
irix_lpsched_exec         IRIX lpsched Command Execution
lssass_ms04_011           Microsoft LSASS MS04-011 Overflow
mailenable_auth_header    MailEnable Authorization Header Buffer Overf
mailenable_imap           MailEnable Pro (1.54) IMAP SELECT Request Buffer
Overflow
maxdb_webdbm_get_overflow  MaxDB WebDBM GET Buffer Overflow
  
```

```

Unreal Tournament 2004 "secure" Overflow (Win32)
War-FTPD 1.65 PASS Overflow
War-FTPD 1.65 USER Overflow
WebSTAR FTP Server USER Overflow
Microsoft SSL PCT MS04-011 Overflow
Microsoft WINS MS04-045 Code Execution
WS-FTP Server 5.03 MKD Overflow
ZENworks 6.5 Desktop/Server Management Remote S
rgets', 'payloads', 'options', or 'advanced'
rgets
  
```



```

msf windows_ssl_pct >
COPYRIGHT © 2003-2005 METASPLOIT.COM
  
```

# Enterprise Protection from Exploits

---

- MUST have streamlined patching procedures
- MUST have an inventory process
  - Include Asset Criticality
  - Include Exposure Levels (inbound & outbound)
- MUST have vulnerability management standards and procedures in place

# Attacking Wireless Networks



# Cracking Wireless Using Freely Available Tools

---

Demonstration

# Wireless Solutions

---

- Strong Authentication
- Strong Encryption
- Protect client systems
- Wireless IPS
- Modern Technologies

# Web Application Targeting

---

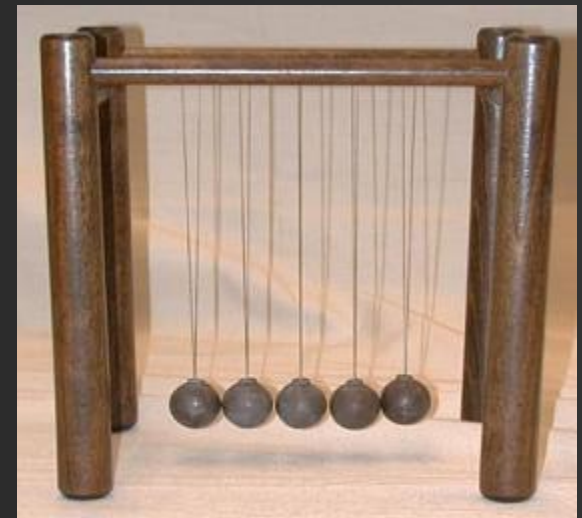
## Manipulating the Way Things are 'Supposed' to Work

- Web Application Attacks
  - On average, 90% of all dynamic content sites have vulnerabilities associated with them.
    - “Today over **70%** of attacks against a company's network come at the 'Application Layer' not the Network or System layer.” - *Gartner*
  - These attacks occur due to the applications inability to prevent a user from modifying data submitted to the site – post-browser / pre-server
    - SQL Injection
    - Parameter Manipulation
    - Session Mgt / Privilege Escalation
    - Error Handling
    - Denial of Service

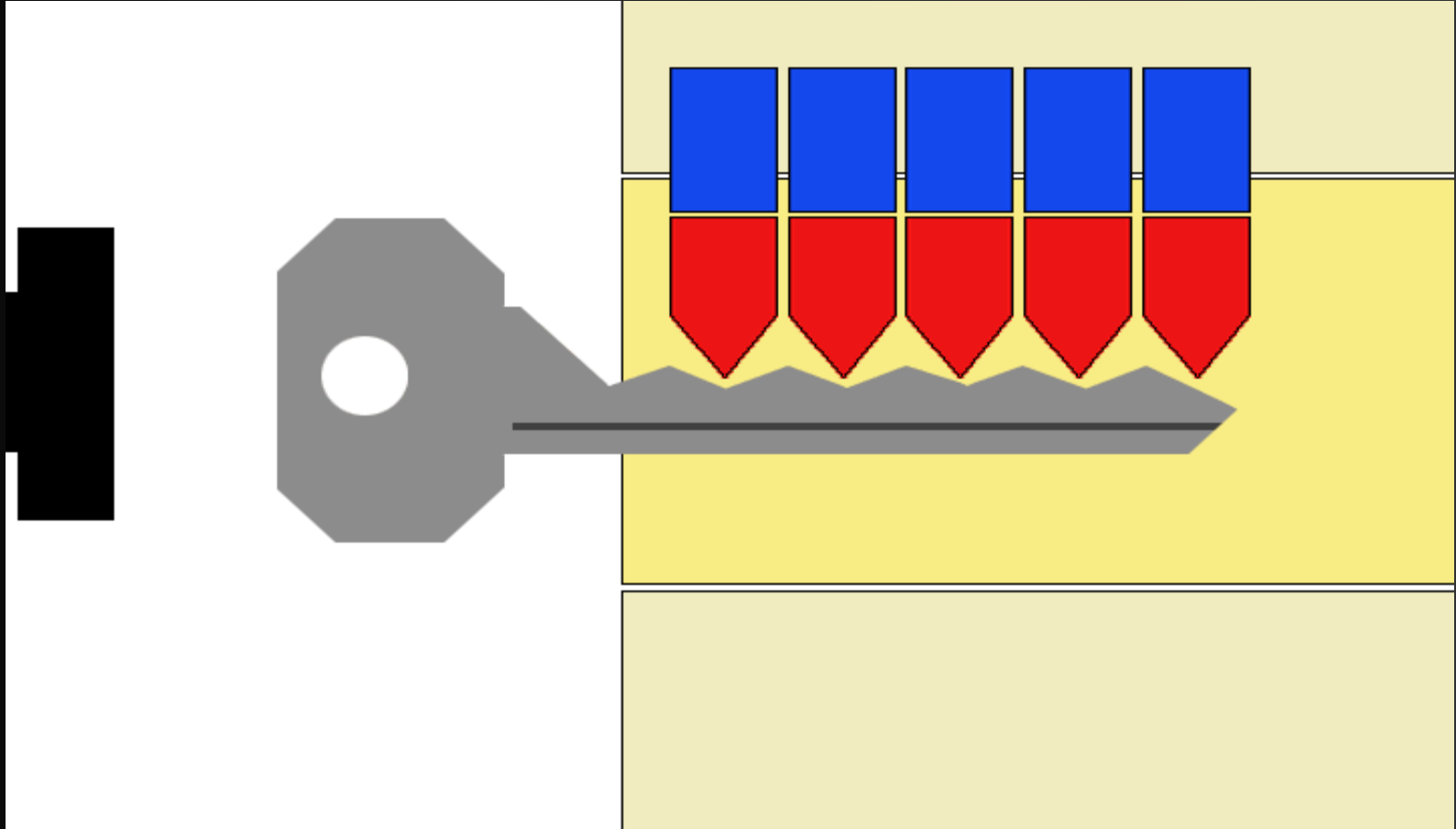
# Physical Security Attacks – Key Bumping

## Physical Access is superior to Network Access

- Bumping Technique –
  - Specialized keys
  - Newton's cradle principle
  - Related to pick gun lock picking method



# Key Bumping

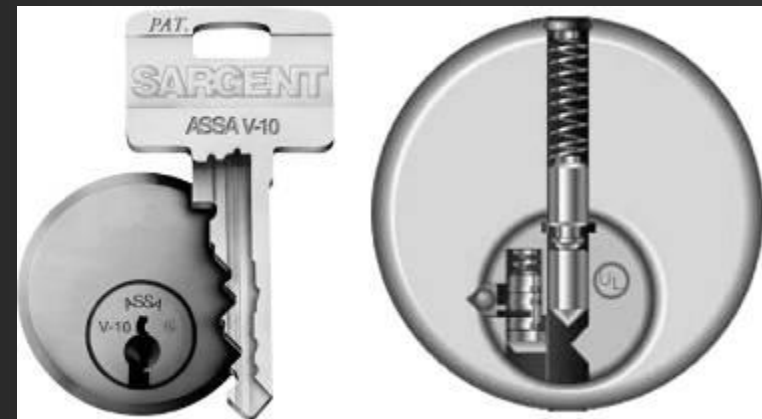


---

# Demonstration

# Key Bumping Threat

- High Level of Risk
  - Inexpensive
  - Inconspicuous
  - EASY
  - Few locks offer protection
  - Insurance problems



# RFID

- RFID has been in use for a while but now is being put into “everything”
- Uses include retail, manufacturing, animal identification, to access control
- Attack Vectors:
  - Asset Tracking / Data Modification
  - SQL Injection (just like web apps)
  - Cloning



---

# Demonstration

# RFID Defense Strategies

---

- Follow the Basics:
  - As with all RF know your footprint and placements.
  - Follow the technology - upgrade when needed
- Avoiding Being a Victim
  - If you can't upgrade to a newer technology (such as I-Class) change out the entry panels with ones that use TAG+Passcode.

# Conclusions

---

- Understanding where the attacks are coming from and where you are vulnerable is the first step to protecting your assets, your customers and your reputation
- Perimeter security requires a clear understanding of the perimeter and where you are exposed
  - Secure Applications
  - Secure Wireless
  - Secure Facilities
  - Defense-in-Depth
- There is no security through obscurity
- Vulnerabilities are coming out faster and exploitation is getting easier

---

# Questions?