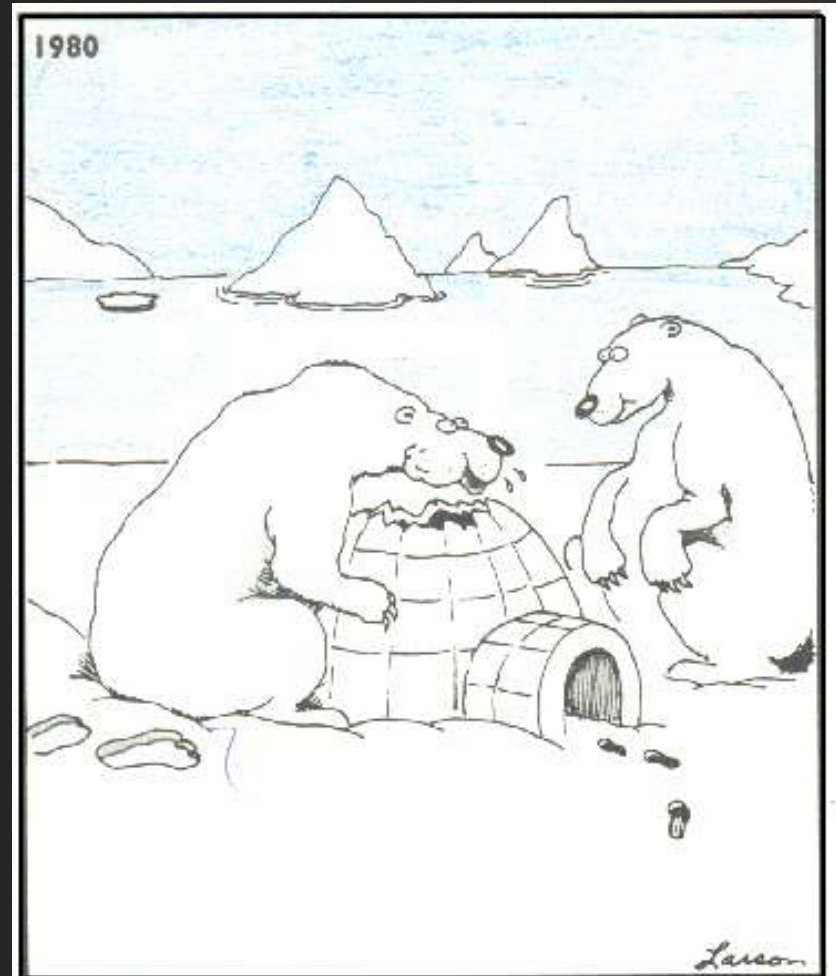


# Current Threats & Countermeasures



## Speakers:

- **David Bonvillain** – Accuvant Director of Assessment Services
- **Jim Broome** – Accuvant Assessment Technical Lead and Principal Assessor



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



# Agenda

---

- The Changing Landscape of Security Architectures
- Modern Attack Vectors
  - Google
    - Data Mining and Target Identification
  - Attack Frameworks
  - Wireless Networks
    - Bypassing Security Controls
  - Web Applications
    - Application attacks from Information Gathering to Exploitation
  - Physical Security
    - Lockpicking for the lazy/efficient
  - VoIP
    - Spoofing, Monitoring and Phishing
  - RFID Hacking
- Solutions and Mitigation Strategies

# Since January 1, 2007...

---

Over 200+ known instances of  
privacy violation via:

- Data Security Breach / Intrusions
- Theft
- Inappropriate Use of Data

# The Information Security Problem

T. Ameri  
Date  
A  
CC  
As C

From Science to Solutions®

## SAIC

Customers | [David Utter](#)

Services & Products | About SAIC

9/14/2007/2  
SAIC 9/14/2007/2  
Security Failure

- Open Letter from the Chairman and CEO
- CEO Letter to SAIC Employees
- News Release
- Questions & Answers

### SAIC Response

20 July 2007

The personal information of found at risk of potential contracts for the Department might cause and offers our to those affected by this se

Nov. 6  
Here a  
amen  
Const  
order,  
electic  
More

### American Sign To Head Off Kais 17,400 Austin Hos. Uni. Competition

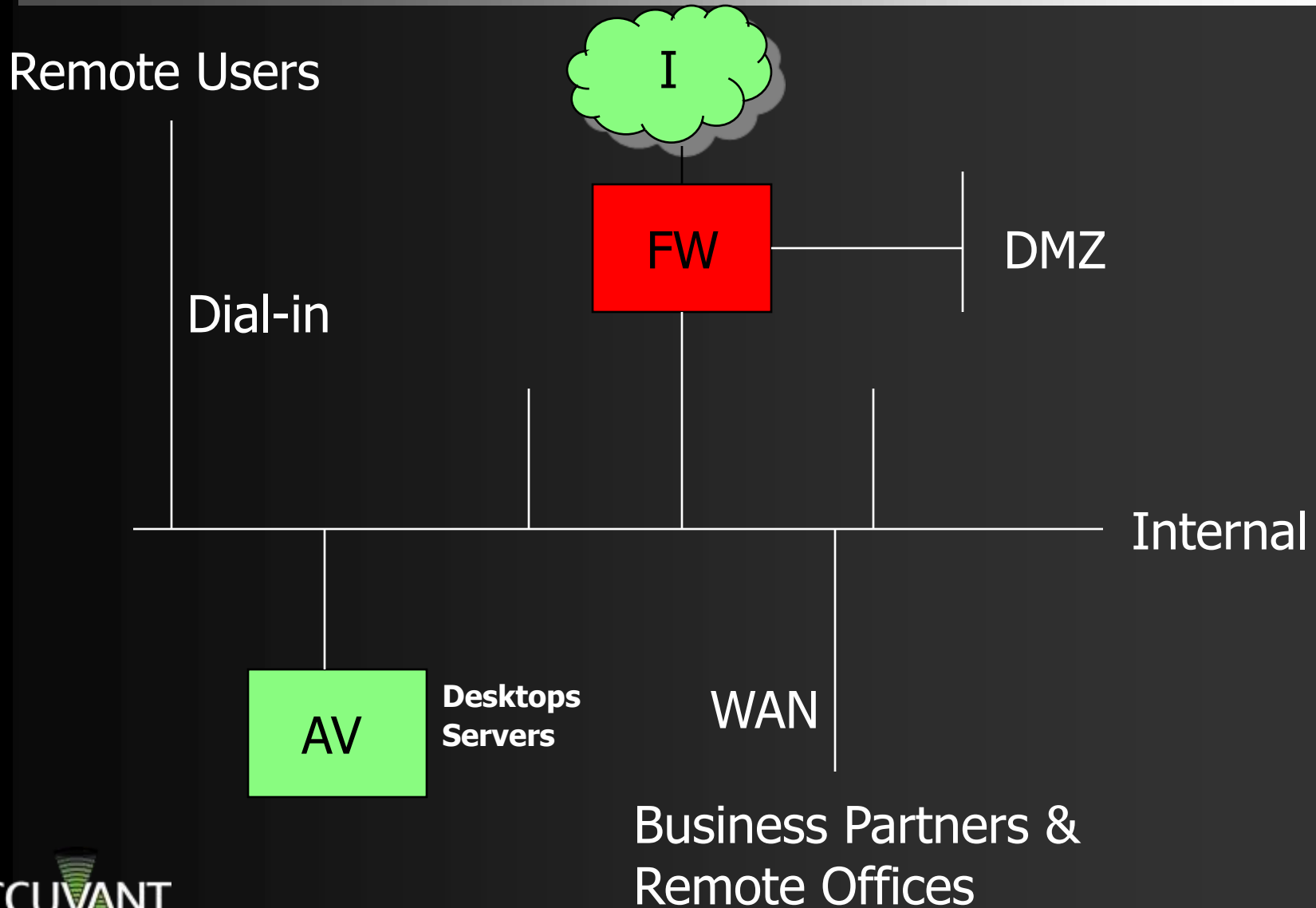
## Fox News Forgets About Directory Security

COMPLETE STORY

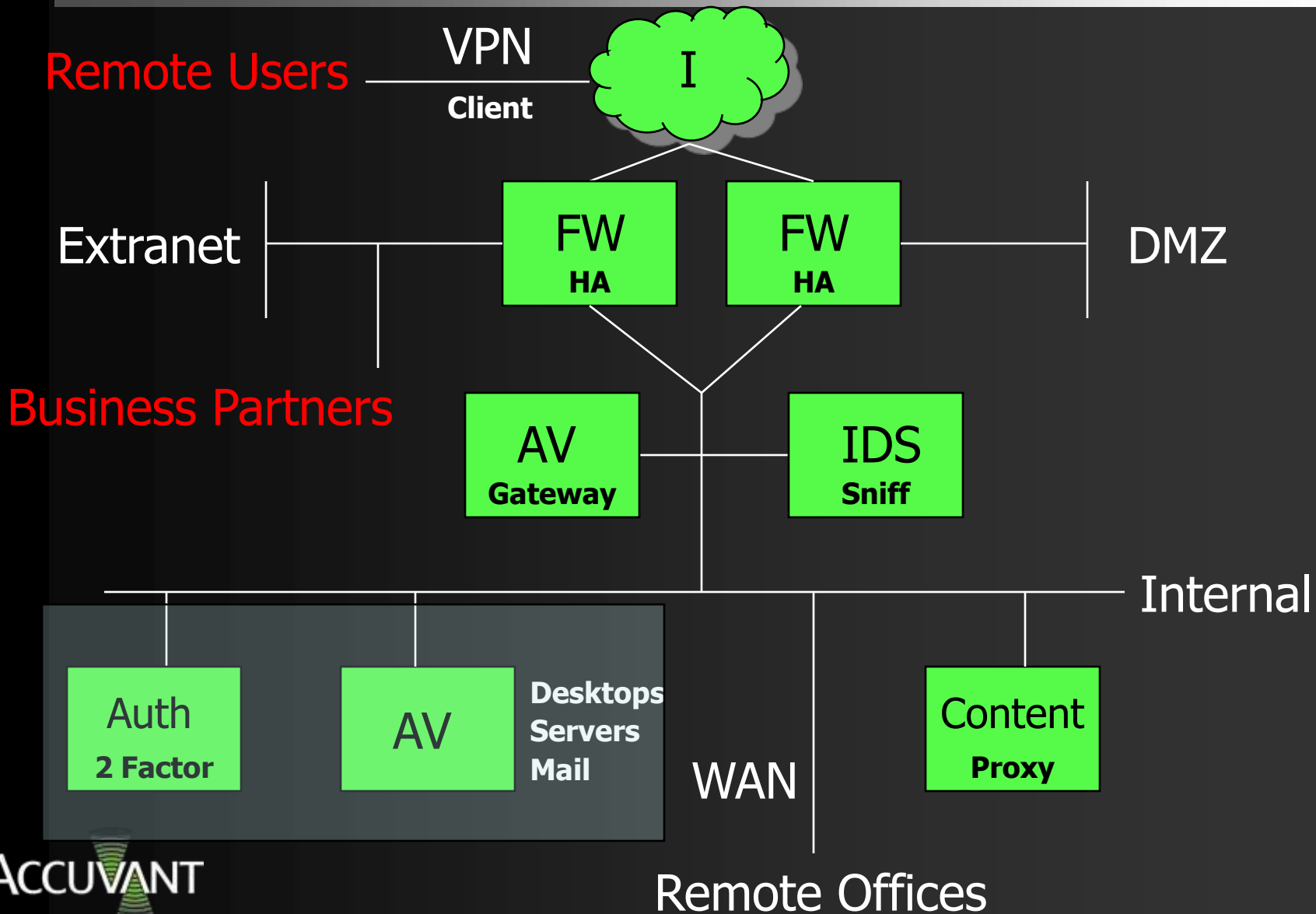
carefully review their credit card and debit card statements and other account information for unauthorized use. We want to assure our customers that this issue has the highest priority at TJX."



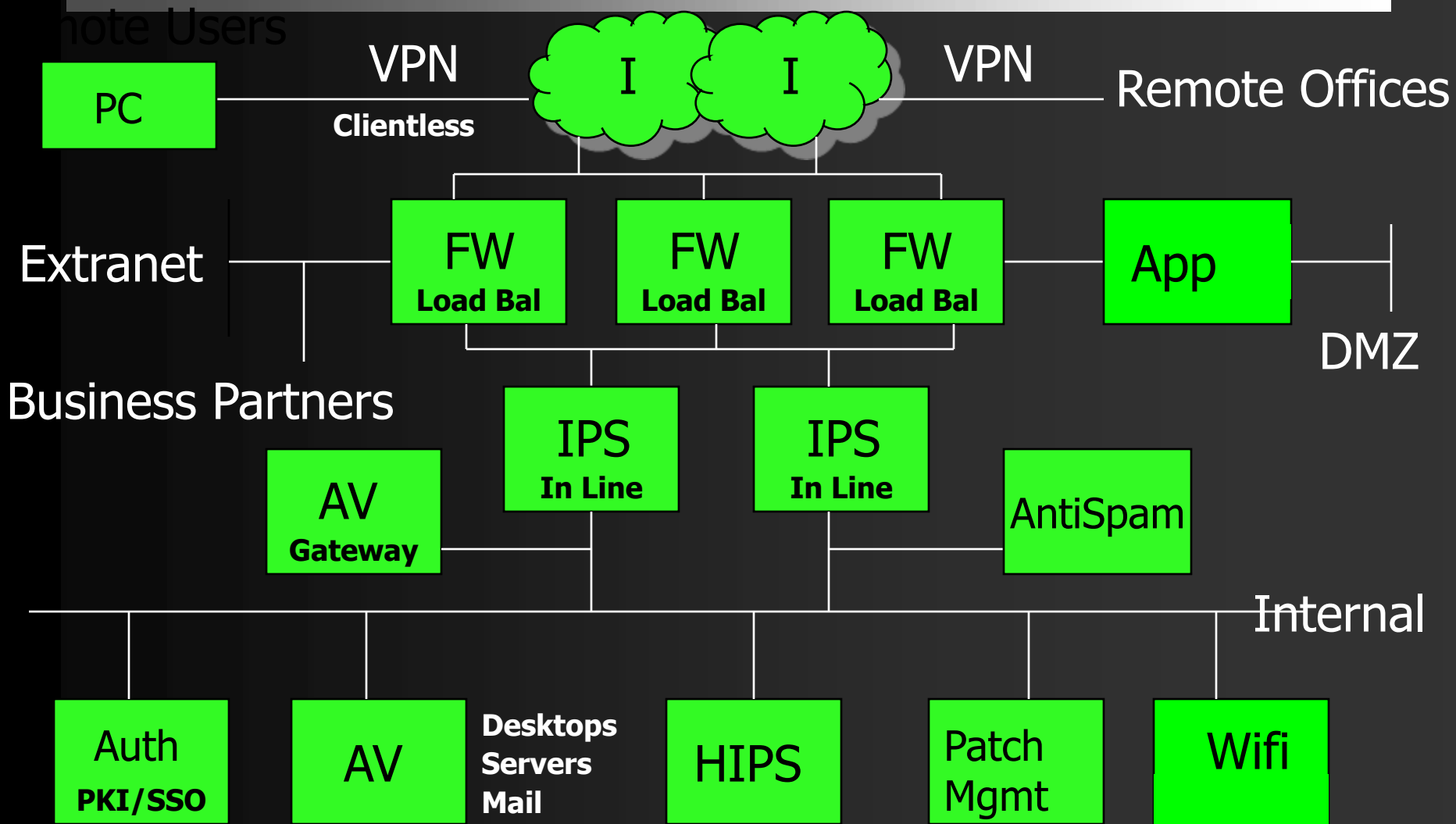
# Security Architecture - 1999



# Security Architecture - 2001



# Security Architecture - 2007

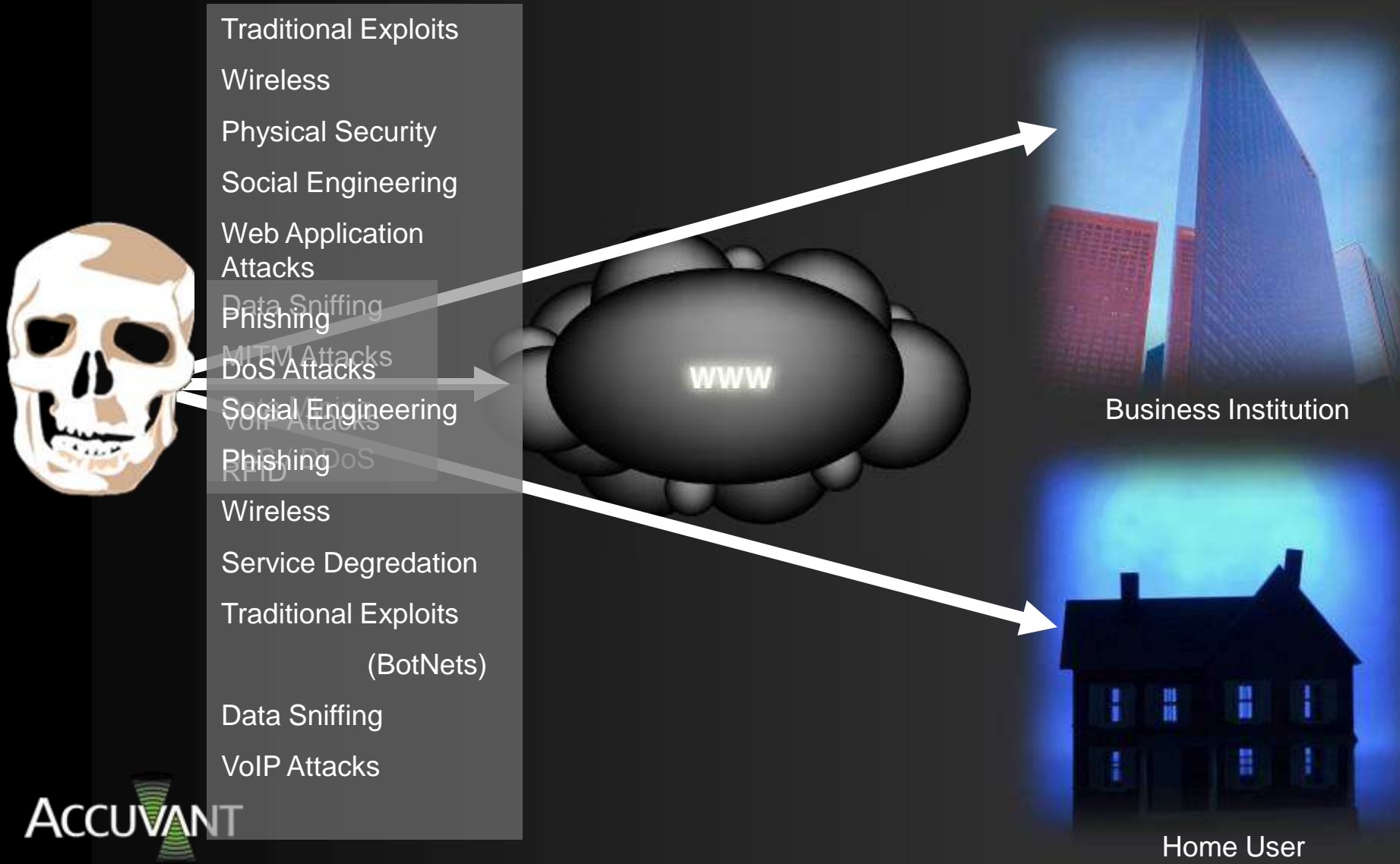


---

As Architectures Have Changed,  
So Have the Hackers Techniques

# Understanding Our Perimeter...

## Where are the Threats?



# Data Mining and Target Identification

---

- Google Hacking
  - Introduced in 2003 by Johnny Long – [johnny.ihackstuff.com](http://johnny.ihackstuff.com)
  - Takes advantage of Google's spidering capability along with finely crafted search queries to find information on the web
    - intitle: | allinurl: | intext: | filetype:
  - Targeting:
    - Sensitive Information
    - Data Mining "Usernames and Passwords"
    - Finding Vulnerable Targets (Error Messages, Banners, etc.)
    - Driver for web application worms

# Using Google to Identify Targets

---

## Demonstration

# You may not be looking for trouble...

---

## Public Data Leakage Solutions

- Never leave unnecessary files on a web server (i.e. Web.config.old, password.log)
- Assume all files on a web server will be seen by a someone with malicious intent
- Encrypt sensitive information in configuration files

# Traditional Exploits Tools & Techniques

- Public Code / Reverse engineering
  - Patch Tuesday = Exploit Wednesday
- Frequently the target of Virus' and Worms
- Exploit Frameworks
  - MetaSploit
  - Canvas (Immunity Security)
  - Mosquito
  - IMPACT (CORE technologies)



# Traditional Exploit Solutions

---

- 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

The image is a composite of two main parts. On the right is a satellite map from Google Maps showing a residential neighborhood. Numerous yellow pushpins are placed on the map, each with a text label identifying a wireless network. The labels include: 'nattynet', 'apolloct', 'chief', 'REIFSNIDER', 'carlos', 'NETGEAR', 'linksys', 'default', 'Christmas', 'ACTION', 'DuncanGS', 'linksys', 'offman10343', 'wireless', 'Raiders', 'no ssid', 'John's Network', 'Home', 'Linksys', 'Ewen's Network', 'DOYLE FAMILY', 'shirebaggins', 'letmein', 'ourhome', 'no current ssid', 'MANDM', 'Carthage', 'default', 'linksys', and 'akde'. On the left is a screenshot of a web browser window displaying an advertisement for 'radio io Jam'. The ad features the text 'radio io Jam' and 'we've listened, we've changed, check it out' along with images of various mobile phones. The browser's address bar shows 'http://www.radioio.com/'. The system tray at the bottom of the browser window shows the time as 21:52 and the date as 12/15. The system tray also includes icons for 'Shell - Koro', 'Interface with', and 'X dnetnet'. The text 'SOCIAT 215' is visible in the bottom left corner, and 'Motorol' and 'Gundan Wing' are visible at the bottom of the image.

# 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

# Application Vulnerabilities

---

Demonstration

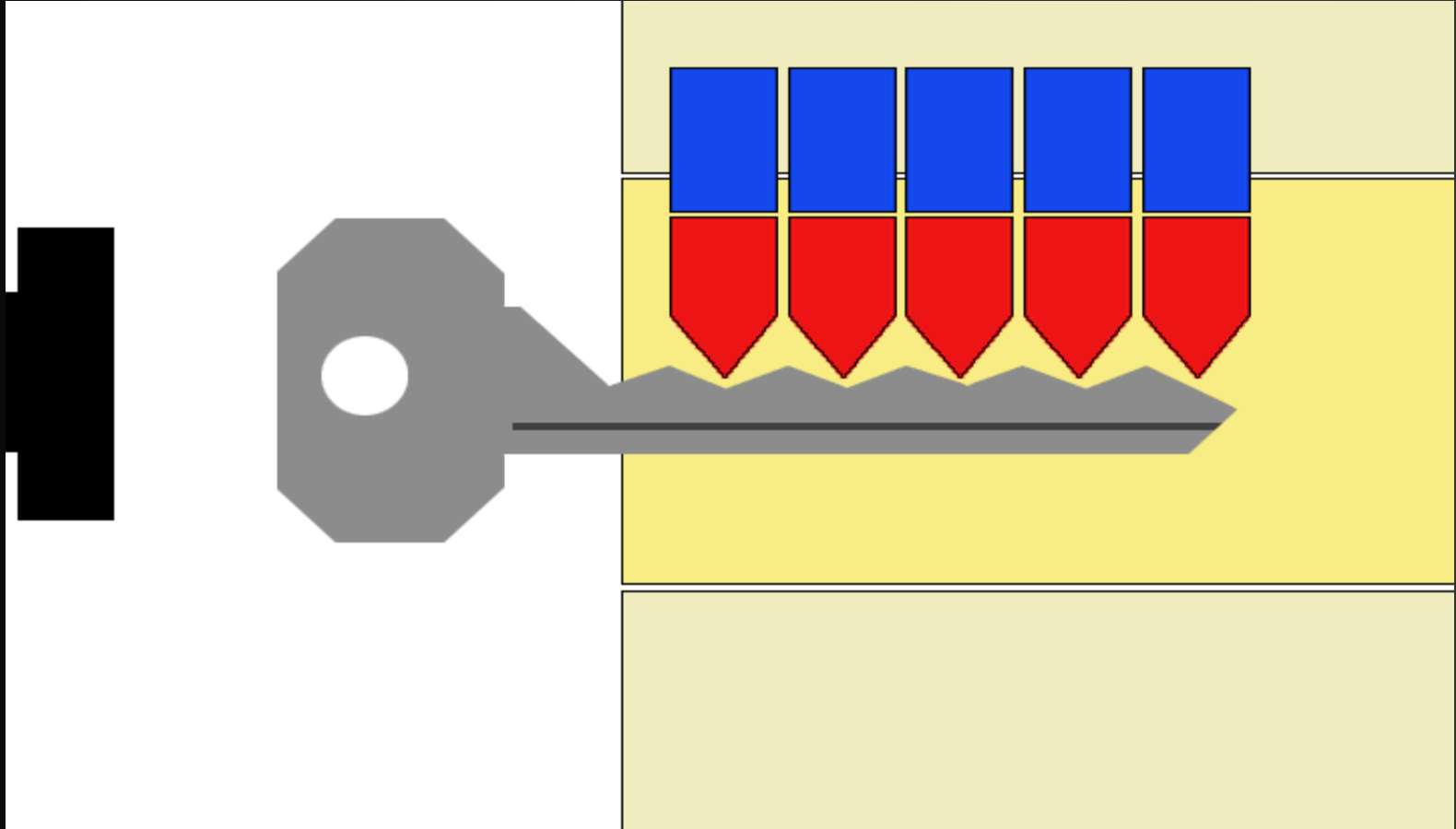
# Physical Security Attacks – Key Bumping

## Once Physical Access is Obtained...It's Game Over

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



# Key Bumping

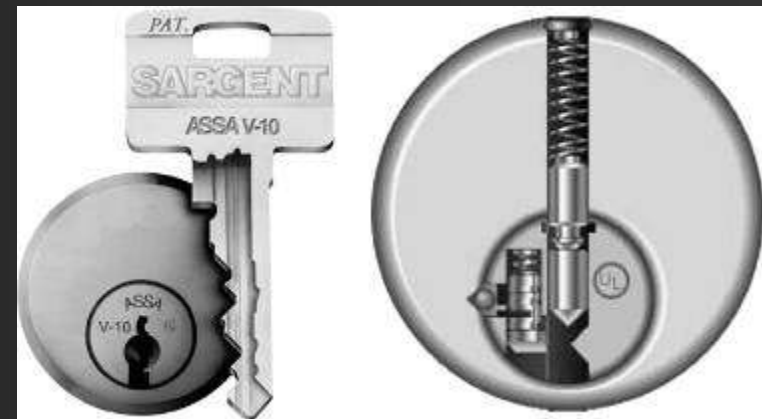


---

# Demonstration

# Key Bumping Threat

- High Level of Risk
  - Inexpensive
  - Inconspicuous
  - EASY
  - Few locks offer protection
    - Especially in the USA
      - Sidebars
      - Trap Pins
      - Shadow Drilling
  - Insurance problems



# VoIP

- VoIP Implementations Becoming Prolific
  - Security / Stability / Availability are Critical for Consumer Experience / Brand Reputation
- With the installation of VoIP solutions, older phone issues are now having to be re-addressed
- Technical Attack Vectors:
  - Traditional Exploits
  - QoS/DoS Attacks
  - Call HiJacking
    - Evesdropping
    - Manipulation
  - VoIP Phishing
    - Identity Theft
- Human Attack Vectors:
  - Caller ID Spoofing
    - VM theft
    - Social Engineering
  - 911 systems



---

# Demonstration

# VoIP Defense Strategies

---

- Follow the Basics:
  - Robust Architecture
  - Defense-in-Depth
- Avoiding Being a Victim
  - Set Passwords on your accounts
  - Never believe Caller-ID
  - Never give out any sensitive information to someone who calls you or as a return call to an un-validated source
  - Validate any information with pertinent institution

# 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?