Spyware NG – How Movies will steal your identity

Robert W. Baldwin, Plus Five Consulting, Inc.
Kevin W. Kingdon, Intellitrove, Inc.

RSA CONFERENCE 2006

Abstract

This presentation may be downloaded from:
http://www.plusfive.com/reports.html or
http://www.intellitrove.com/presentations.html or
RSA Conference web site

Abstract

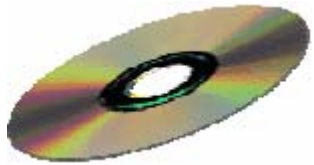
Next generation spyware will be able to hide inside movies, audio and video delivered over the Internet. Come learn how advanced features in video formats enable this new spyware delivery channel.

A lively dialog examines whether this new threat means the end of the electronic entertainment or is just another round in the fight between attackers and defenders.

You decide whether the “sky is falling”.

Are Videos a new Threat Vector?

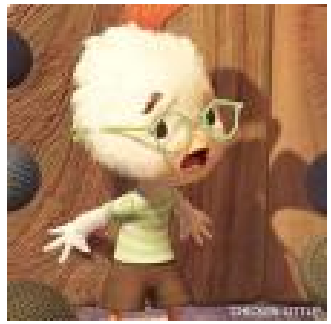
- Today: Inserting DVD in PC launches applications
  - Needed to install latest player
  - Needed to install games and related services



- Consumers don't expect threats from entertainment appliance
  - Appliance has all the powers of a network PC
  - Fortunately good engineering has kept out the worst threats

What about Tomorrow?

- Malware embedded in video
- Recent events
- Overview of formats and device features
- What helps and hinders security?
- Threat to the enterprise?
- Convergence on single platform vs. Divergence of many appliances
- Our Predictions



Issues Behind Video Security Goals

- Consumers enjoy content at acceptable price
  - My video, Anywhere, Anytime
- Distributors make money on content
  - Home, Lodging, Airplanes, Wireless
- Electronics vendors make money on CE hardware
  - New features drive new sales
- Lots of secondary revenue
  - Advertisements and purchase for digital merchandise
  - On-the-Go shopping for non-digital merchandise

Are Videos a new Threat Vector?

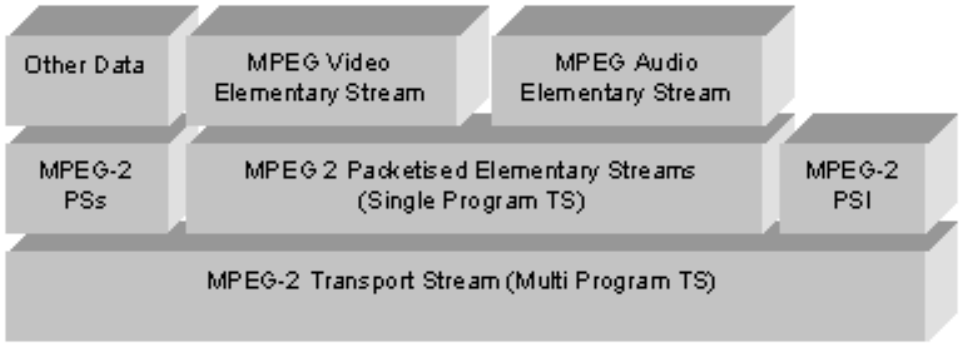
- Attacks delivered when movies played
- Same threat can come from
  - E-Mail, and animated E-Greeting cards
  - Instant Message file sharing
  - Clicking on web pages
- Firewalls, virus scanners and spam filters could handle these
  - Hopefully this talk will encourage security vendors
  - Anti-Piracy features likely to make filtering harder

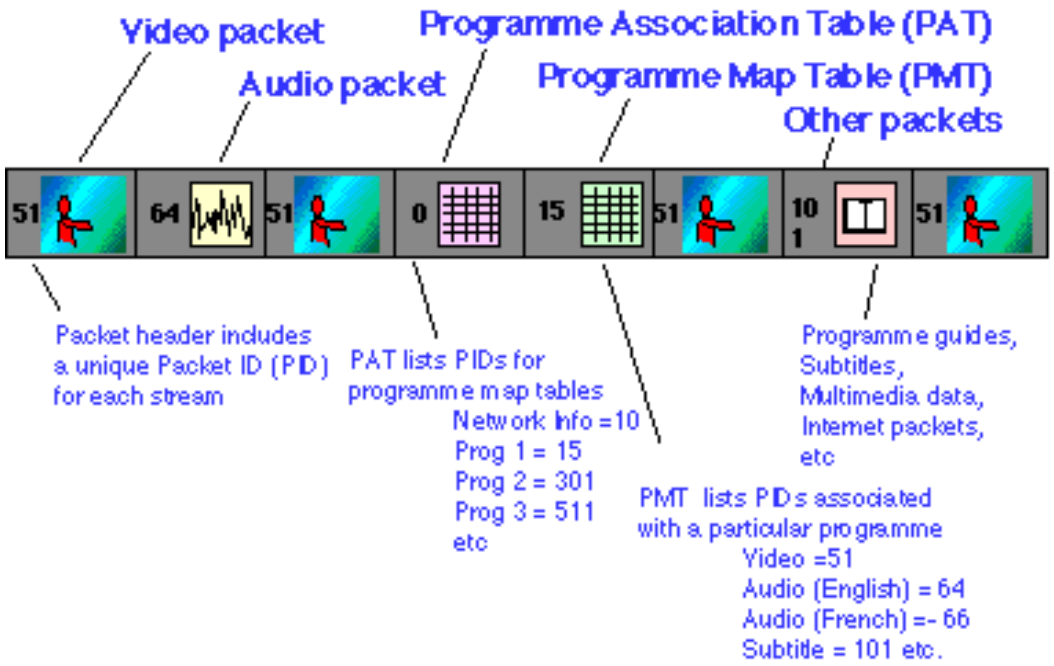
Recent Events

- Security software for content protection subverted by bad guys
  - Root kits stealth features being used by other spyware
  - Nasty public relations problem
- Still encountering major security flaws
  - Mono culture: PC & MPEG are attractive targets
  - Demand for features discourages Security
  - Cost of flaws not born by software or device vendors
- Good news is that these problems are found and fixed
  - Scary problem if patching NOT allowed

Video & Audio Formats

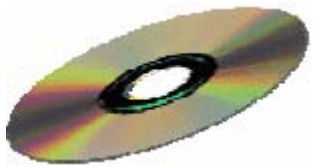
- H.261 Video Conferencing
- AVI, QuickTime, MPEG2
  - MPEG4 Extensible, DRM





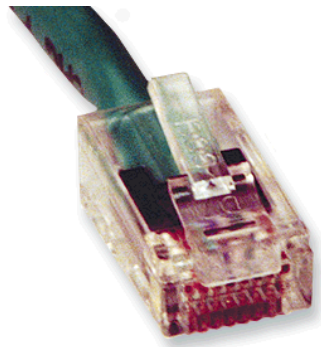
AV Delivery Infrastructure

- Digital Video Broadcast GEM
- MHP Executable
- Blu-Ray, HD-DVD
- Internet



Advanced Features of Devices

- Features of newer CE equipment.
  - High bandwidth networking
  - Bulk storage of content
  - Auto install
  - Auto update
  - Anti-piracy features (can be dangerous)
  - Persistent storage of consumer information



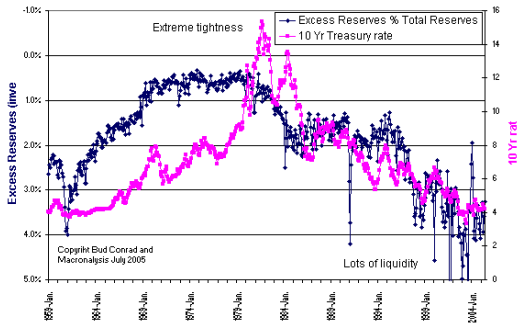
- Internet access via any available path
  - Game box searching for open wireless access point

Attacks on Formats, Codecs, and Devices

- Flaws will be discovered in seldom implemented variants
  - In-band markers, audio-only, unusual frame-rates
- The “old reliable” – buffer overflows
- Send multiple packet streams to the same set-top “channel”
- Deliberately drop frames of various types
- Attacker’s content will violate the MPEG2 and MPEG4 rules
  - Frame-type ordering rules, Frame-type ratios, Malformed packets
- Attacker Goal: If you can crash the set-top, you can exploit it
- Market pressures discourage good security

Market Pressures Favoring Security

- Market pressures that increase security?
  - Conformance tests, especially 3rd party
  - Intellectual Property barriers to keep out untrustworthy vendors
  - Methods to limit damage caused by untrustworthy vendors



- Responses
  - Studio specific responses to attacks
  - CE vendor specific responses to attacks
  - Multi-vendor responses to broad attacks

What Helps Security?

- Trusted sources of content and related links
  - Trusted clickable links
- Closed distribution chain helps security
  - Walled gardens: DVD brand name vendor, Trusted cable operator
  - iTunes vs. Google video
- TiVo or Cable TV DVR connected to Internet
  - TiVo to Go – Now the channel has non-trusted elements
- Rely on trusted intermediaries to protect consumer
  - Credit card companies, PayPal, Amazon
  - Trusted vendors of software
  - Trusted vendors of video content (Discs, Satellite, DSL and IP)

What Helps Security?

- What technologies can help security?
- Sandbox good: Java, GEM, Flash
- Less ID info in box is good
- Fewer options to reconfigure
- Media is interpreted
  - Can be good
  - Can be bad (WMF)

What Helps Security?

- Existing security tools still helpful
  - Deep understanding of formats
  - AV, Filters, Firewalls, Anti-spam
  - Spyware scanners
  - Windows Update

- Anti-Piracy features can conflict with filtering
  - Filters need access to decrypted content

What Helps Security?

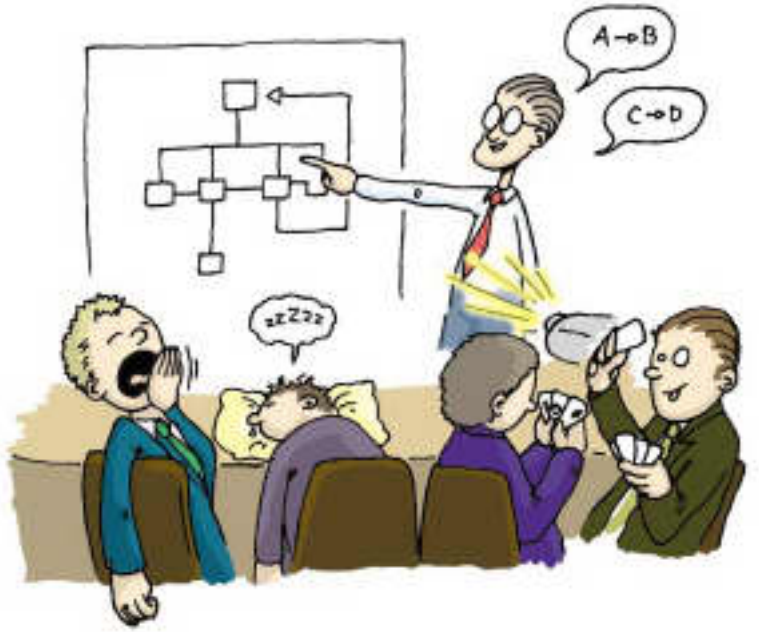
- Install permanent patch – Necessary but scary
  - To appliance firmware
  - To local copy of media
- Temporary patching vs. permanent changes
  - Double-edge sword
  - Bad guys could use patches to install spyware
- Compromises Possible
  - Patch until Reset button pressed
  - Patch until power cycled
  - Restore previously good state (new for CE)

Main Points Thus Far

- Better entertainment features conflict with Security
  - Less attention from product marketing
  - Less from product designers
  - Less attention from QA
- The economy goes on
  - A large group of consumers will pay the CE vendors and content owners and content distributors for good value received
- Huge benefit from vendors thinking like the bad guys
  - Focused review of security design
  - Penetration testing. Start early in QA cycles.

Enterprise Security Problem?

- This IS an enterprise problem!
- Video is becoming a mainstream presentation format
  - High value impact in a 5 second clip from famous movie
- User don't think about music and video as storage vector
  - Un-patched systems can be infected when content played



Enterprise Security Problem?

- Two stage delivery: USB or video iPod can be carrier
  - Device driver code runs when device plugged in
  - Auto install features might provide all the required access
  - Auto install bugs could provide additional access
- Multi stage attack
  - Home PC exploit infects consumer's video transcoder
  - Infected transcoder spreads virus to ALL recordable media
  - Media shared via work
  - Virus recognizes work environment, begins active spreading
  - Entire workplace could become infected

Appliance vs. Platform?

- Divergence by appliance user interface, or Convergence on universal platform?
- We predict: Divergence
  - Gaming machine
  - Entertainment machine
  - Office desktop or Laptop
  - PDA
  - Fax / Copier / Scanner
  - Phone
  - Digital camera

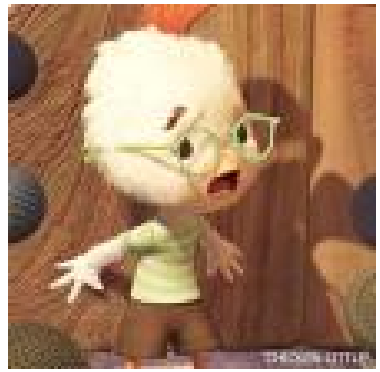
Appliance vs. Platform?

- Features of User Interface drive Divergence
  - Telephone UI is great
  - Gaming machine UI is great
  - Office PC UI is great
  - Entertainment center UI is OK
  - Fax / Copier / Scanner UI is great
  - Movie and still camera UI is great
- Prediction: Divergence will win
- Prediction: Entertainment appliances will dominate the home

Plus Five Consulting
and
Intellitrove

Worse Case Predictions

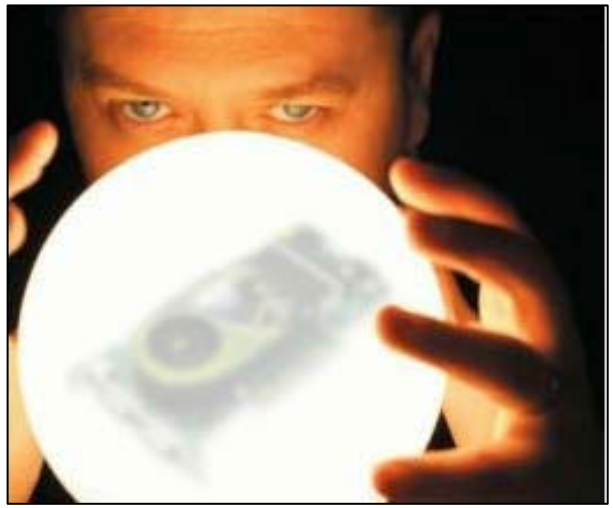
- Bad guys harness the storage and network bandwidth of hundreds of thousands of drone PCs
  - Many pieces of video assembled to thwart watermarking
  - Drones perform brute force cracking of Subscriber IDs, Watermark system, DRM setting, perhaps even Movie Title keys



- Drones install spyware to gather:
  DRM licenses (new), Credit card numbers & Home banking info
- Drones create geographically distributed caches of movies that can provide local high bandwidth access
  - Bad guys can charge subscription fee for this service!

Predictions

- Discs go away (or become disposable)
  - File servers and Fast downloads
  - Bulk sharing with friends via short fiber optic cable



- Reputation systems grow
  - Easier to find trustworthy vendors
  - Reviews automated and integrated with buying step
- Fear of attacks will reduce piracy of content

Our Recommendations

- Consumers and IT managers ask your security vendors about this
- Make the security of device part of your purchasing decision
  - This is the only way to encourage good security design & QA
- Future is hopeful, but keep an umbrella nearby

Additional Resources

- http://www.plusfive.com/
- http://www.intellitrove.com/
- http://www.tomshardware.com/1999/09/24/video_guide_part_3/
- http://www.dvb.org
- http://www.mhp.org
- http://www.blu-ray.org/