Content Protection and Security Considerations for 5G

KILROY HUGHES

2015.08.20

5G Content Protection and Security Topics

1. **Is that a computer in your pocket?**
   (or, are you just happy to see me? – Mae West)
2. **DRM Beyond HD Video**
   DRM changes for UHD, HDR, WCG, VR, etc. video; and tighter control of all content in an environment of ubiquitous networking
3. **Internet of Things**
   Software security becomes more difficult and higher risk

Computer in Your Pocket, Data in the Cloud

- Today I can set a Windows 10 phone on a pad, and it will wirelessly connect to a large display with full computer workstation functionality and hundreds of gigabytes of personal cloud storage accessible from any device I use
  - Like wireless charging, market forces and standardization will eventually drive interoperability (Miracast, DLNA, AirPlay, etc.)
- Mobile devices are becoming an authentication mechanism to access your data and "AI" in the cloud
  - Now used for 2 factor Auth, virtual smartcard/SIM, but evolving to biometric ID
  - "Hello Windows" is an example of UI independent user identification (multifactor, voice, face, gesture, other biometrics and secrets beyond PIN and password}
- Many portable and wearable devices will have useful computation capacity, but the cloud has infinite resources
  - If a device can uplink clicks, gestures, voice, video, etc., the cloud can downlink the result of teraflops and petabytes of computation.
  - The user experience can be human communication like Skype, AI communication like Cortana and Siri, enterprise apps like Office, video games, virtual reality, enhanced reality, plain old video and music, etc.

DRM Beyond HD Video

- 5G enables UHD video, which has spawned **next generation DRM**
  - But, content providers and services may require next gen DRM on all HDR content, all early window content, etc. considering the business impact of ubiquitous 5G high bandwidth global access if that content leaks
- Next Gen DRM
  - Example: PlayReady 3, Security Level 3000
  - Built into hardware, like Qualcomm chips, or enforced by hardware in a trusted execution environment and trusted video path (e.g. Win10, all software signed and verified by root of trust, hardware contained keys). DRM running in a browser or other app is insufficient. EME talks to hardware DRM.
  - Separate encryption keys, licenses, and policies for audio, SD, HD, and UHD video. Output controls can require HDMI 2 for UHD.
  - Stringent robustness rules and certification prior to deployment and DRM device key issuance. Contractual enforcement is the primary trust mechanism (non-technical).
  - Active management: Breach tracking via watermarks, key revocation, renewal, "patch Tuesdays", hundreds of security experts review all code, threat models, attack testing, etc.
  - Fingerprints proposed: Each device generates a unique audio and/or video output so unauthorized video can be traced to a specific device and that device revoked
  - Trusted DRM identity and rights expression language used for new business models, entitlements, and authorization methods (e.g. broadcast, continuous live TV channels, etc.)

Securing the Internet of Things

- Critical infrastructure will be 5G networked (cars, doors, cameras, watches, toasters, elevators, air conditioning, power grid, centrifuges, toilets …)
  - Subject to code injection that can collect personal info, damage devices (Stuxnet), crash cars, etc.
  - Zombie armies that are not monitored like PCs, phones, etc. can attack other network resources and services (DoS attacks, etc.)
- Mobile and wearable devices network your location, health, personal information, contacts, audio, video, etc. (https://allseenalliance.org)
  - The "app model" of portable software is convenient, but "sandbox security" isn't adequate
  - Trusted execution environment isn't the direction IoT is going (a million variants of open source software in devices)
  - TLS link protection might help Man in Middle attacks, but broadcast/multicast breaks that
- Compare to DRM:
  - What is the trust model, contractual enforcement, robustness rules, cryptographic identity management, revocation, renewal, antivirus, firewall, malicious software removal, etc. active security model for IoT? Who monitors and manages it (beside the NSA)?