The zombies you watch or play in video games on your smart TV may be less scary than the abilities of hackers using the same device. Researchers from NCC Group's iSEC Partners will go into depth about the vulnerabilities of smart televisions at EE Live! 2014, in a talk titled "The Outer Limits: Hacking a Smart TV."

"Smart TV attacks are increasing, and, similar to smartphones, they have a large attack surface... which we have only scratched," said Aaron Grattafori, principal security engineer and research lead with iSEC.

Grattafori and Josh Yavor, iSEC senior security engineer, will speak at EE Live! about their research into susceptible Samsung smart TVs. Their research has been focused on two 2012 Samsung televisions, but they say designs are similar across major market models.

"We pretty quickly discovered that there wasn't a great design in terms of security," Grattafori said. "It's very easy to write a malicious application that would take files off the TV and access the camera without you even knowing it. We even took that further and found existing vulnerability in applications that would allow us to hijack them." It was actually "very, very easy to remotely compromise the TV."

Yavor and Grattafori were able to work against the web browser, steal files, and infect other applications that affect the television itself. The applications they hacked have since been fixed, but the researchers also found issues with TV versions of Skype and Facebook applications.

Problems occur when the television manufacturer writes major social applications, and the app owners provide only a small library of code for functionality, often allowing basic security measures to be overlooked. For example, a hacker could send a message or change a mood status on Skype generating code which, when viewed, would give complete remote control of the application.

"Any time that there is a nonstandard OS, there are a lot of security issues that happen, and companies need to be diligent about performing testing or internal auditing," Grattafori said. "Lots of work needs to go into those to make sure that there aren't malicious applications and that all security applications work as intended."

In order to beef up security and make hacking harder, Grattafori encouraged developers to be aware of known web bugs and strengthen requirements on usernames to prevent the use of malicious code.

The two were also able to hack the front-facing camera, which Grattafori called mostly a "scary factor." The Samsung TVs don't use an LED to notify users when the camera is on, so hackers could use the camera without being noticed. In response, Samsung issued a press release suggesting that..."
users rotate and tuck the camera into the bezel of the TV for security.

LG's smart TVs accidentally log file names of USB drives and channels watched, Grattafori said. Such privacy issues will become a future problem.

He compared the level of security on today's smart TVs to that of smartphones and computers several years ago. "Things are getting better but there is a long road ahead."

Aaron Grattafori and Josh Yavor's talk will be part of the EE Live! Black Hat Security Summit on Thursday, April 3.

Attend the session The Outer Limits: Hacking a Smart TV on April 3 at EE Live! 2014. Follow updates about EE Live! programs and sessions on Twitter, Facebook, LinkedIn, and Google+ and register for the March 31-April 3, San Jose-based event here until Thursday, March 27, 2014, or in person at the event.

EE Live! is managed by UBM Tech, EDN's parent company.

Also see:

- Qualcomm Snapdragon 802 powers smart TVs
- Far-field voice processor enhances smart TVs
- X-box hacker Andrew “Bunnie” Huang to keynote at EE Live! 2014
- EE Live! 2014