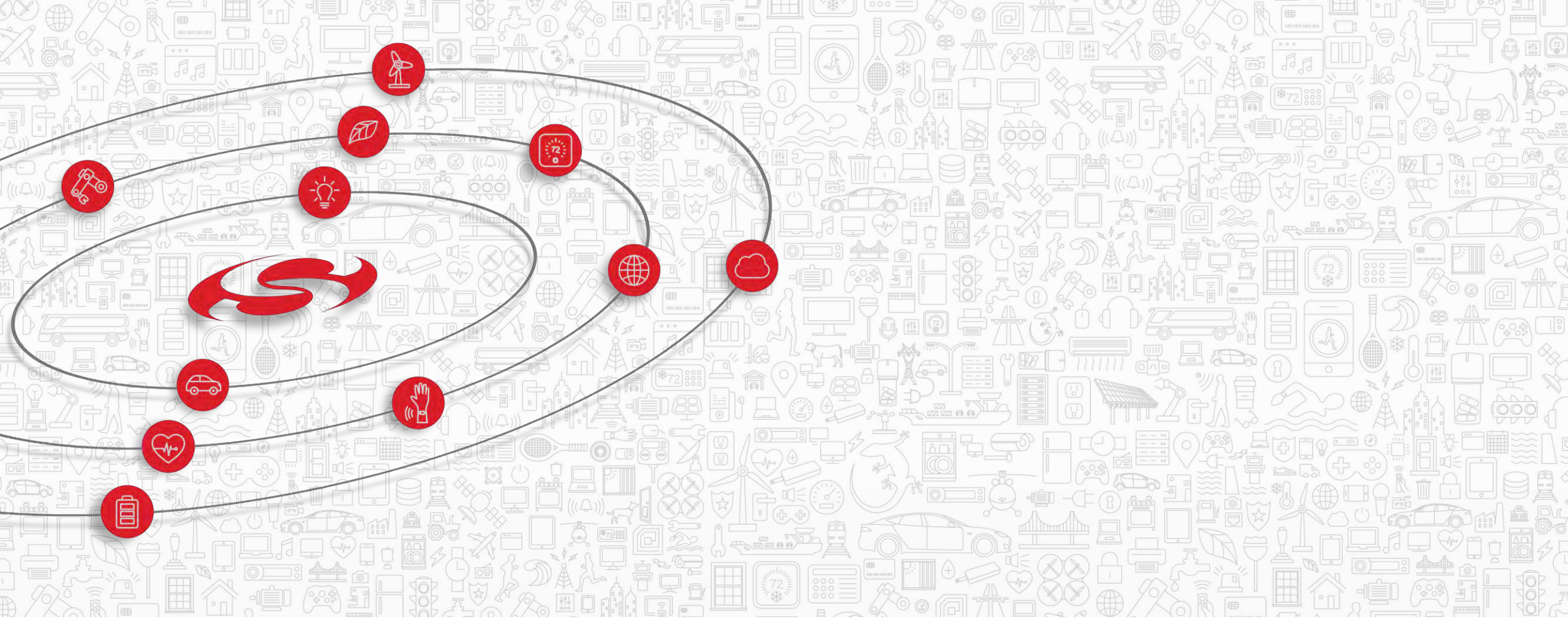
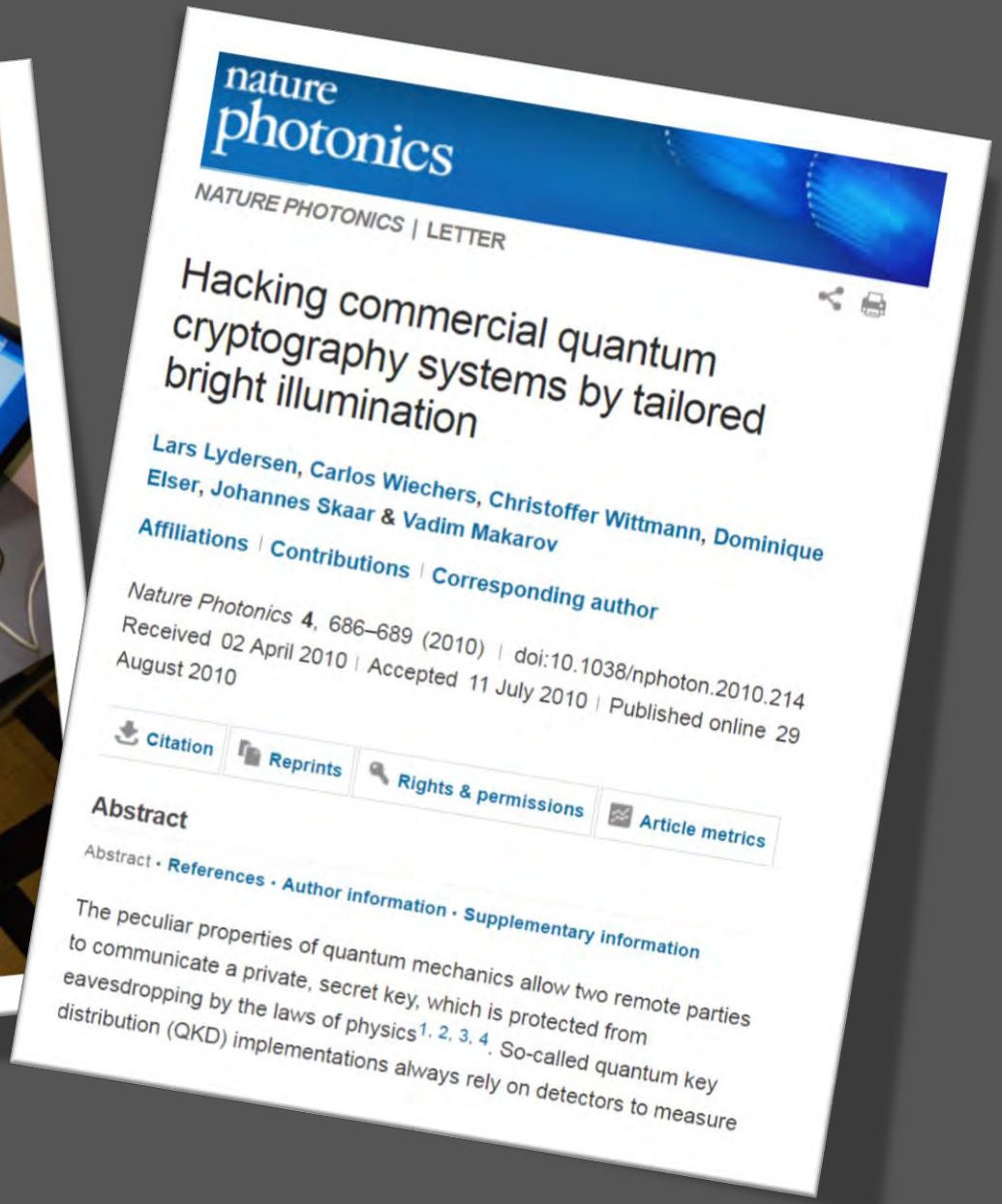


Security in the IoT

Lars Lydersen | 08 Mars 2017

SILICON LABS

Meet Lars the Quantum Hacker



nature photonics

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Affiliations | Contributions | Corresponding author

Nature Photonics 4, 686–689 (2010) | doi:10.1038/nphoton.2010.214
Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

Citation | Reprints | Rights & permissions | Article metrics

Abstract

Abstract · References · Author information · Supplementary information

The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics[1, 2, 3, 4]. So-called quantum key distribution (QKD) implementations always rely on detectors to measure

Press

LE FIGARO·fr

Le journal

Premium Actualité Economi

LE FLASH ACTU 14h34 Brexit: la Grèce menace de bloquer un accor

Réputée inviolable, l
été

ACTUALITE > SCIENCES ET TECHNOLOGIES (ARCHIVES)

LE FIGARO PREMIUM
1 mois d'essai offert
sans engagement

LES AUTEURS
SUR LE MÊME SUJET
RÉAGIR (31)
PARTAGER
IMPRIMER

新华网
WWW.NEWS.CN

新华新闻 新闻中心 > 正文

挪威发现“无痕截

2010年08月31日 11:31:52 来源：新

新华网伦敦８月３０日电（记者黄
通信接收方的探测器会很快发现。但挪威研
上报告说，他们找到一种“无痕截获”量子
况下获得通话内容。

在微观世界里，不论两个光子等粒
一个粒子，这种现象叫量子纠缠。量子通信
通信方式。从理论上说，无法在观测一个量
的窃听是肯定会被发现的。

但挪威科技大学等机构的研究人员
信接收方发出一束特殊的激光，这束激光可
有传统光学探测器的功能。因此，只要窃听

Frankfurter Allgemeine Zeitung, 2010-09-08

Listige Attacke auf den Quantenschlüssel

Verwundbare Kryptographie: Clevere Hacker knacken einen vermeintlich sicheren Quantencode und zeigen damit zwei kommerziellen Systemen ihre Grenzen auf.

Von Manfred Lindinger

Ob beim Online-Banking, beim Einkauf im Internet oder beim Austausch internen Firmenwissens und von Bankgeheimnissen – vertrauliche Informationen sollte man stets verschlüsselt weitergeben, damit sie nicht in falsche Hände geraten. Trotz aller Bemühungen lassen sich Nachrichten mit klassischen Verschlüsselungsverfahren aber noch immer nicht sicher übertragen. Einen Ausweg verspricht die Quantenkryptographie, die zum Austausch vertraulicher Informationen die Prinzipien der Quantenphysik nutzt. Dadurch sollte das heimliche Abhören so gut wie unmöglich werden. Doch auch diese Technik scheint offenkundig ihre Schwachpunkte zu haben, wie eine deutsch-norwegische Forschergruppe nun zeigen konnte.

Herkömmliche Verschlüsselungstechniken beruhen darauf, dass bestimmte Rechenoperationen wie die Primfaktorzerlegung nur mit großem Rechenaufwand ausgeführt werden können. Doch mit fortschreitender Computertechnik wird es wahrscheinlicher, dass jeder als sicher geltende Code in kürzester Zeit geknackt werden kann. Anders bei der Quantenkryptographie. Bei dieser Technik wird nicht die Botschaft selbst übermittelt, sondern eine zufällige Folge von binären Nullen und Einsen, die als Schlüssel dient. Erst mit diesem Schlüssel kann der Empfänger („Bob") die eigentliche Nachricht des Senders („Alice") lesen. Der Clou des Verfahrens ist, dass ein Spion – „Eve" –, der die verschlüsselten Informationen „abhört", diese selbst merklich verändert,

BB84-Protokoll genannt – übermittelt Alice an Bob eine zufällige Folge von Nullen und Einsen in Form einzelner Lichtteilchen mit insgesamt vier verschiedenen Polarisationen. Als „Null" und „Eins" werden dabei die jeweils senkrecht zueinander polarisierten Schwingungszustände interpretiert.

heitliches Quantensystem verhalten. Die Forscher verschränkten die Photonen des Senders mit Lichtpulsen, die sie als potentielle Abhörer erzeugten. Auf diese Weise hofften sie, unbemerkt an Informationen über Schwingungszustände der Lichtteilchen zu gelangen und den Quantenschlüs-

TON.2010.214) berichten, haben sie dazu gezielt einen technischen Schwachpunkt von Bob ausgenutzt: seine Detektoren.

Zum Nachweis schwacher Lichtpulse oder einzelner Photonen werden üblicherweise sogenannte Lawinenphotodioden verwendet. Diese sind extrem empfindli-

Schneier on Security

Blog Newsletter Books Essays News Speaking Crypto About Me

← Cyber-Offence is the New Cyber-Defense UAE Man-in-the-Middle Attack Against SSL →

Successful Attack Against a Quantum Cryptography System

Clever:

> Quantum cryptography is often touted as being perfectly secure. It is based on the principle that you cannot make measurements of a quantum system without disturbing it. So, in theory, it is impossible for an eavesdropper to intercept a quantum encryption key without disrupting it in a noticeable way, triggering alarm bells.
>
> Vadim Makarov at the Norwegian University of Science and Technology in Trondheim and his colleagues have now cracked it. "Our hack gave 100% knowledge of the key, with zero disturbance to the system," he says.
>
> [...]
>
> The cunning part is that while blinded, Bob's detector cannot function as a 'quantum detector' that distinguishes between different quantum states of incoming light. However,

Search

Powered by DuckDuckGo

Go

blog essays whole site

Subscribe

About Bruce Schneier

Bruce Schneier today

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

Security

Bruce Schneier: We're sleepwalking towards digital disaster and are too dumb to stop

Coders and tech bros playing chance with the future

Fear ... Bruce Schneier (Photo © Rama, Cc-by-sa-2.0-fr)

2 Mar 2016 at 21:38, Iain Thomson 358 809

digi.no

IT-sikkerhetseksperten Bruce Schneier, her avbildet under Congress on Privacy & Surveillance (CoPS213) ved Ecole Polytechnique Federale de Lausanne. Foto: Rama, Wikimedia Commons, Cc-by-sa-2.0-fr

INTERNET OF EVERYTHING

Ingen kan forutsi konsekvensene av tingenes internett

Men det verste vi kan gjøre, er å få panikk, sier sikkerhetsguru.

Recent press #1: Mirai botnet attacks

WIRED SUBSCRIBE

LILY HAY NEWMAN SECURITY 12.09.16 7:00 AM

THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY

- IP-camera's and DVRs have telnet backdoors exploited by "Mirai"
- End user cannot close backdoor
- Source released; anyone can get a botnet
- Used to attack a number of targets including DYN
- Gained massive attention

Recent press #2: A lightbulb worm?

COMPUTERWORLD FROM IDG

INSIDER Sign In | Register

SECURITY IS SEXY

By Darlene Storm | Follow

About

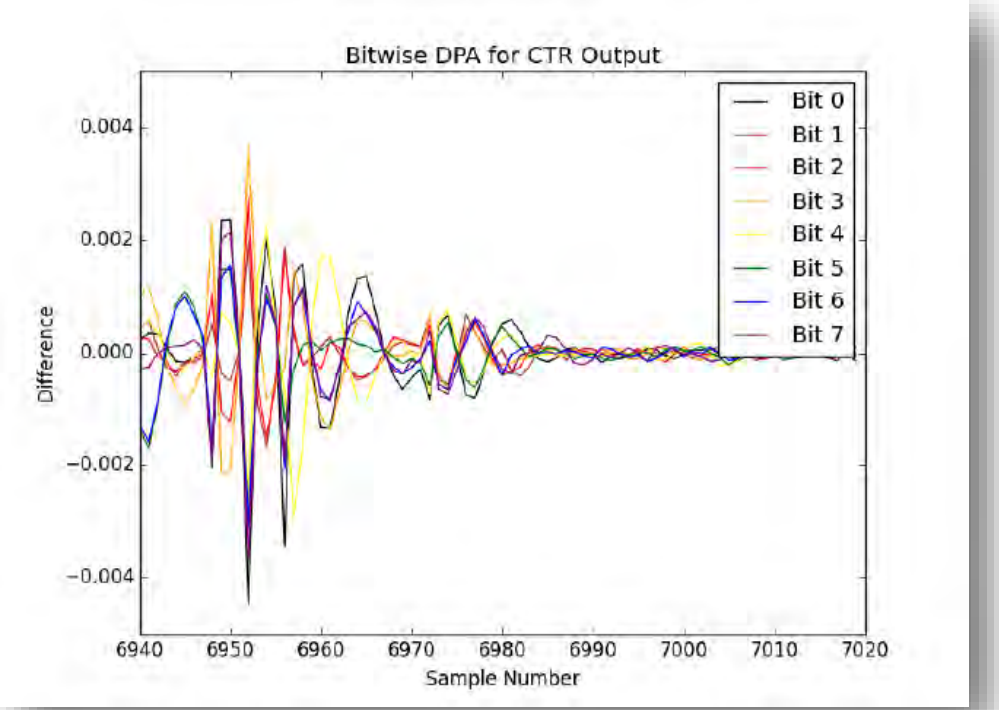
Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Researchers hack Philips Hue lights via a drone; IoT worm could cause city blackout

Researchers hijack Philips Hue lights with a drone to show how IoT worm could take over smart lights in a city.

Computerworld | NOV 9, 2016 7:39 AM PT



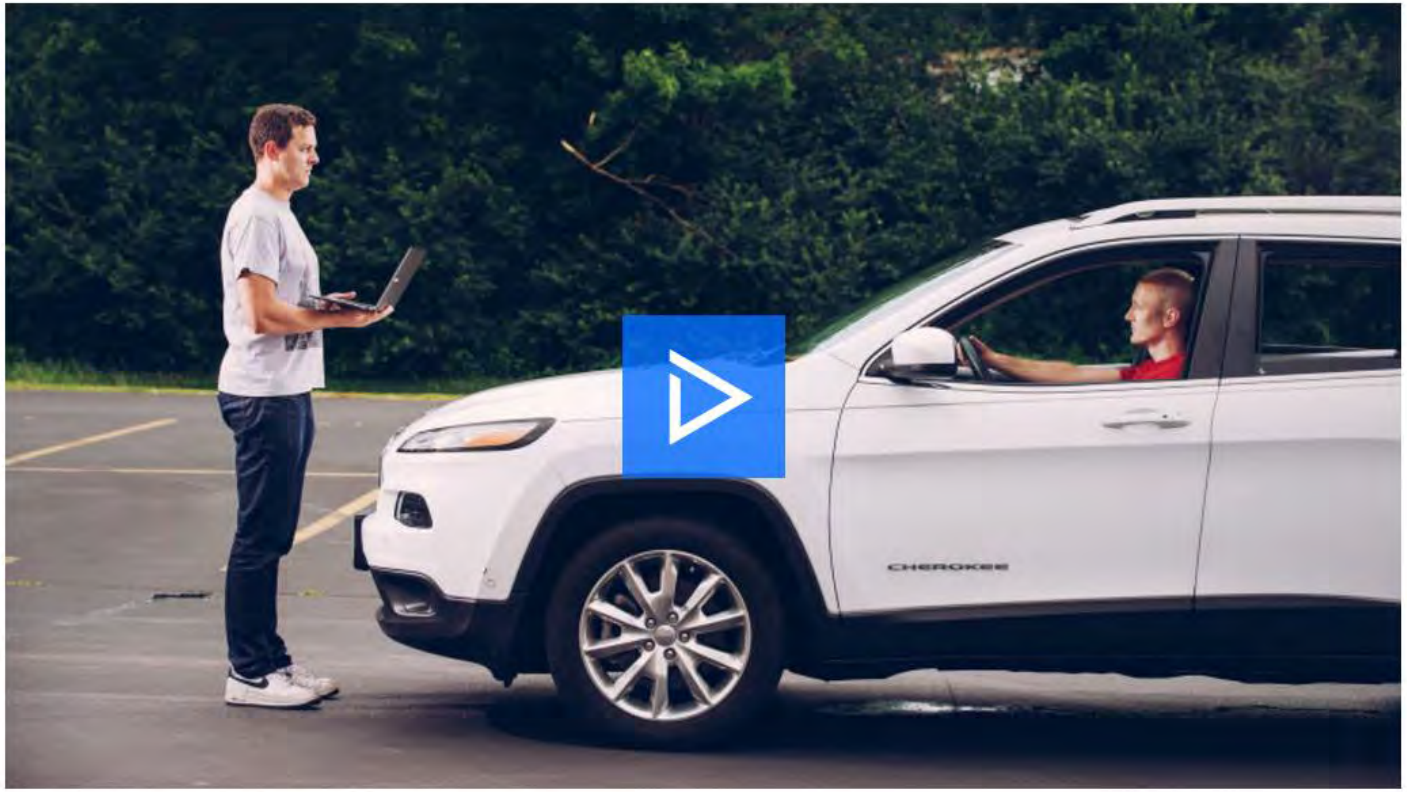
Philips hue	ID: 24158E Model: BSB002 Version: 01035934
6. Hue color lamp 1	Model: LCT001 Version: IrradiateHue
7. Hue color downlight 1	Model: LCT002 Version: 5.23.1.13452

WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It SUBSCRIBE

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY | TRANSPORTATION

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



WIRED

HACKERS CAN DISABLE A SNIPER RIFLE—OR CHANGE ITS TARGET

Smart Engineers

What you see

You aimed here

The gun shot here