**SAMPLE SUBMISSION**

**Title:** HTTP/2: The Sequel is Always Worse

*Submitted by: James Kettle, PortSwigger Web Security (Black Hat USA 2021)*

**Abstract (Provide a concise, yet detailed description of your presentation - 300 word maximum):**
HTTP/2 is easily mistaken for a transport-layer protocol that can be swapped in with zero security implications for the website behind it. Two years ago, I presented HTTP Desync Attacks and kicked off a wave of request smuggling, but HTTP/2 escaped serious analysis. In this presentation, I'll take you beyond the frontiers of existing HTTP/2 research, to unearth horrifying implementation flaws and subtle RFC oversights.

I'll show you how these flaws enable HTTP/2-exclusive desync attacks, with case studies targeting high-profile websites powered by servers ranging from Amazon's Application Load Balancer to WAFs, CDNs, and bespoke stacks by big tech. I'll demonstrate critical impact by hijacking thick clients, poisoning caches, and stealing plaintext passwords to net multiple max-bounties. One of these attacks remarkably offers an array of exploit-paths surpassing all known techniques.

After that, I'll unveil novel techniques and tooling to crack open a widespread but overlooked request smuggling variant affecting both HTTP/1 and HTTP/2 that is typically mistaken for a false positive.

Finally, I'll drop multiple exploit-primitives that resurrect a largely-forgotten class of vulnerability, and use HTTP/2 to expose fresh application-layer attack surface.

I'll leave you with an open-source scanner with accurate automated detection, a custom, open-source HTTP/2 stack so you can try out your own ideas, and free interactive labs so you can hone your new skills on live systems.

*Notes:*

- *Detailed, yet concise abstract*
- *Defines a problem and offers a solution(s) that will be examined during the session.*

**Presentation Outline (Show the progression of your presentation.)**

Brief outline:

- Introduction & core-concept explanation
- HTTP/2-exclusive desync attack techniques with case studies
- Request tunneling techniques with case studies and a tool live-demo
- Misc. HTTP/2-exclusive attacks
- Defense & Takeaways

Detailed Outline:

- I'll open with the 2-minute story of this research's origin, including how it's a year late because I was initially fooled into thinking HTTP/2 was secure.
- Then I'll briefly introduce the concept of HTTP/2 downgrades (front-ends that convert HTTP/2 requests from the client into HTTP/1 requests for the back-end), and show how this enables desync attacks. This will

function as a very quick request smuggling recap as I'm assuming most audience members will already be familiar with the topic.

- The first core section will use case-studies to illustrate HTTP/2-exclusive desync attacks that enable cross-user exploitation. These case studies include:
  - Simply sending an incorrect Content-Length header over HTTP/2 for zero-interaction account hijacking on netflix.com, earning a maximum $20,000 bounty.
  - Using fake chunked encoding over HTTP/2 to exploit numerous systems running Amazon's Application Load Balancer. I'll focus on two particularly interesting case studies, earning $7k and a maximum $10k.
  - Combining a desync attack with Ruby on Rails framework features to directly steal plaintext passwords from a compliance provider
  - Using CRLF in header values to inject extra headers for full takeover of every site using the Netlify CDN.
  - Using a HTTP/1-impossible header name to exploit a major online retailer, and cache poison every site using a popular cloud WAF.
- After that I'll explore request tunneling, which is a more constrained subtype of HTTP desync attacks that enables internal header spoofing and therefore still has potential for critical impact. This section will:
  - Show how although Amazon's HTTP Desync Guardian mitigates normal desync exploitation techniques, it fails to prevent request tunnelling.
  - Introduce a groundbreaking new approach that makes many desync-powered request tunneling vulnerabilities non-blind.
  - Live-demo a Param Miner extension that uses this technique to detect hijackable internal headers
  - Revisit a technique mentioned earlier and show how it can be used for 'complete request splitting'.
  - Show how this powerful new primitive can be combined with application functionality to directly disclose internal headers (this case study is a WIP)
  - Show how complete-request-splitting can be combined with the non-blind tunneling technique to escalate request tunneling into cache poisoning, which is otherwise impossible. I'll use a well-known SaaS vendor as a case-study.
- In the final core section I'll present some novel exploit primitives/gadgets that HTTP/2 provides. This section won't include full exploitation case studies but every primitive has been confirmed to work on multiple live systems. Each of these is built on the way HTTP/2 violates multiple assumptions that held in HTTP/1.1.
  - The request scheme is now user input, enabling request line injection attacks. Also, the path and method can now contain raw spaces, enabling the same.
  - It's now possible to send multiple paths on one request, and there's even more ways to specify the Host ambiguously.
  - An obscure RFC trick can be used to append content to internal headers
  - If I find a proper case study in time, I'll also demonstrate the potential for cross-protocol desync attacks on SMTP.
- Next I'll explore how to recognize and avoid some pitfalls I've encountered including vulnerable servers that pretend not to support HTTP/2, or exhibit stream-dependent behaviour.
- Then I'll discuss some approaches to defense for server-implementers, RFC authors, and anyone who wants to use HTTP/2 for their application.
- I'll wrap up with the key takeaways, leaving five minutes for questions.

*Notes:*

- *Clearly conveys progression of talk.*
- *Helps the Review Board visualize the presentation in its entirety.*
- *Gives an explanation of each area of the presentation.*

**Attendee Takeaways (What are three actionable takeaways included in your presentation?)**

1. The HTTP/2 spec is so complex that implementers frequently skip security-critical steps.

2. However, the spec is also careless about violating assumptions present in HTTP/1.1 so spec-compliant implementations are often exploitable.
3. As a result, although HTTP/2 aspires to be a transport-layer wrapper around classic HTTP semantics it bleeds upwards to enable both server-level and application-level attacks.

*Notes:*

- *Submitter fulfilled requirement of providing 3 takeaways*
- *Explains relevance to the audience*
- *Cleary emphasizes the participant benefits*

**SAMPLE SUBMISSION**

**Title:** Government-Mandated Front Doors?: A Global Assessment of Legalized Government Access to Data
*Submitted by: Andrea Little Limbago, Interos (Black Hat USA 2021)*

**Abstract (Provide a concise, yet detailed description of your presentation - 300 word maximum):**
Who needs a backdoor when front door access is required? From Tesla to the U.S. tech giants, there has been growing focus on whether private sector companies are obliged to turn over data to a foreign government in exchange for market access. This can take the form of source code reviews to unfettered access upon request and increasingly may pose a risk to intellectual property and personal data as digital authoritarian frameworks proliferate.

This comes at a time when significant supply chain disruptions have prompted many in the private sector to reassess their global footprint, with cybersecurity a top priority and motivator when exploring greener pastures elsewhere. Integrating government data access policies must become core to these considerations as corporations reshore and transform their global footprint.

But how do these policies compare from one country to the next? Has the GDPR inspired more progeny or is the Chinese model spreading faster as many contend? To address these questions, this presentation will introduce a new global index of countries based on government-mandated data access requirements. We will discuss the data and factors driving the index, as well as elicit community recommendations for improving the model. With such significant global transformations underway, government-mandated data access warrants greater attention when exploring the full range of global cyber risks.

*Notes:*
*•Detailed, yet concise abstract*
*•Defines a problem and offers a solution(s) that will be examined during the session.*

**Presentation Outline (Show the progression of your presentation.)**
I. Introduction
a. Common adage that tech outpaces policy, but there are significant policy shifts across the globe
b. With the growing Splinternet/Balkanization of the internet and digital and physical supply chains, I was curious how this was playing out with regard to government-mandated data access. Are companies reshoring from one high security risk location to another when it comes to government access to data?
c. Are Russian mandatory source code reviews and Chinese local data storage and security reviews an anomaly or spreading to other regimes? What about Australian backdoor legislation or data protection similar to that found in the GDPR?
d. Building on and integrating the growing literature on encryption, cross-border data flows, and the techno-dictator/digital democracy archetypes, I created a global ranking of government access to data. This talk will share the findings and seek collaboration and feedback to continue to help improve the index and highlight this shifting landscape.

II. Shifting regulatory landscapes in context -
a. The rise of data protection laws and individual data rights - GDPR and its global offspring
b. Data sovereignty - growing requirements to store data locally and/or provide government access to data
c. The various motivations -> national security largely the underlying justification achieved through various means
d. Variations in implementation with examples - ranging from mandated certificates and unfettered access to transparent and limited access with a warrant

III. Why this matters for supply chain resilience
a. Quick overview of the stats and growth of reshoring and onshoring over the last few years

IV. The Model Framework
a. Rankings coded and based on a range of factors:
1) Degree of data localization and storage requirements
2) Degree of legalized government access -> from no access to unfettered access
3) Transparency of government access
4) Joint venture requirements for a local presence
5) Source code access requirements
6) The existence of a federal data protection law and independent data protection authorities

V. The Findings
a. Global country rankings
b. Interesting trends or non-intuitive results
c. All summarized in a white paper

VI. Next Steps
a. Gather feedback from the community for improvement
b. Iterate on the analysis by end of the year
c. Motivate broader thinking about the range of cyber risks and data protection considerations as globalization transforms

*Notes:*
- *Clearly conveys progression of talk.*
- *Helps the Review Board visualize the presentation in its entirety.*
- *Gives an explanation of each area of the presentation.*

**Attendee Takeaways (What are three actionable takeaways included in your presentation?)**

1) Government-mandated access to data poses a growing risk across the globe
2) Rethinking cyber risk to include government policies is increasingly necessary and introduces new risks to IP and PII
3) As supply chains transform and reshore, government data policies should be a top cyber consideration when assessing locations

*Notes:*
- *Submitter fulfilled requirement of providing 3 takeaways*
- *Explains relevance to the audience*
- *Cleary emphasizes the participant benefits*

**SAMPLE SUBMISSION**

**Title:** Can You Hear Me Now? Remote Eavesdropping Vulnerabilities in Mobile Messaging Applications

*Submitted by: Natalie Silvanovich, Security Engineer, Google (Black Hat USA 2021)*

**Abstract:**

On January 29, 2019, a serious vulnerability was discovered by multiple parties in Group FaceTime which allowed an attacker to call a target and force the call to connect without user interaction from the target, allowing the attacker to listen to the target's surroundings without their knowledge or consent. While this remarkable bug was soon fixed, it presented a new and unresearched attack surface in mobile applications that support video conferencing. This presentation covers my attempts to find similar bugs in other messaging applications, including Signal, JioChat, Mocha, Google Duo, and Facebook Messenger.

*Notes:*

- *Detailed, yet concise abstract*
- *Defines a problem and offers a solution(s) that will be examined during the session.*

**Presentation Outline**

- Introduction
  - Explain FaceTime bug that caused call to be answered without user interaction
  - Goal: determine how these bugs happen and could they occur anywhere else
- WebRTC
  - What is WebRTC? (the video conferencing library used by most apps other than WhatsApp and Facetime)
  - How does WebRTC signaling work? What needs to happen for a microphone or camera to send content
- Analysis techniques (How to determine whether an app uses WebRTC and what the state machine looks like)
  - Documentation
  - Frida
  - Reversing with IDA or apktool
- Results
  - Signal and Facebook Messenger bugs
  - Both of these bugs allow audio to be transmitted without user consent
  - Both of these bugs occur due to not checking whether the software is in the correct state before moving to the next one
  - Mocha and JioChat bugs
  - Both bugs occur due to developers not understanding WebRTC functionality
  - Both bugs allow both audio and video to be transmitted without user consent
  - Google Duo bug
  - Occurred due to bad threading
  - Allowed the camera to take photos and transmit them with no user interaction
- Conclusions
  - Basically, everything I looked at had a similar bug to the Group FaceTime bug

- Root causes are lack of attention to security in design, lack of understanding of video conferencing bugs and lack of understanding of this type of vulnerability
- A lot more research is needed

*Notes:*

- *Clearly conveys progression of talk.*
- *Helps the Review Board visualize the presentation in its entirety.*
- *Gives an explanation of each area of the presentation.*

**Attendee Takeaways (What are three actionable takeaways included in your presentation?)**

1. Security researchers should investigate calling state machines when looking for bugs
2. Developers should be careful when implementing calling state machines as they are very vulnerability prone
3. Application design is very important to how these bugs work, and small changes can go a long way in preventing these types of bugs

*Notes:*

- *Submitter fulfilled requirement of providing 3 takeaways*
- *Explains relevance to the audience*
- *Cleary emphasizes the participant benefits*

**SAMPLE SUBMISSION**

**Title:** 5G IMSI Catchers Mirage

*Submitted by: Ravishankar Borgaonkar, Senior Research Scientist, SINTEF Digital & University of Stavanger (Black Hat USA 2021)*

**Abstract (Provide a concise, yet detailed description of your presentation - 300 word maximum)**
IMSI catchers aka Stingrays aka fake base stations are well-known privacy threats to almost every mobile phone with SIM card connectivity (including iOS or Android-based) in the world. The cellular network generations such as 2G,3G, and 4G are vulnerable to such almost undetectable and silent attacks. Finally, new security mechanisms in the next generation 5G networks have been added to address these types of issues. In this talk, we carefully investigate new security protection techniques in 5G and perform practical experiments using commercial 5G devices. Besides, we explain our failure and successful attempts at building 5G IMSI catchers for our research. Finally, we conclude with results explaining what will be the impact of 5G IMSI catchers against 5G users without downgrading to legacy networks; guidelines for the cellular device vendors, operators, and end-users; directions towards fixing the problem in 6G networks.

*Notes:*

- *Detailed, yet concise abstract*
- *Defines a problem and offers a solution(s) that will be examined during the session.*

**Presentation Outline (Show the progression of your presentation.)**

1. IMSI catchers - what/how/why
   In this part, we explain the IMSI catcher threat and the state-of-the-art in attack techniques. Tracking and interception over the radio access network will be covered. In particular, how the problem started in 2G to carried way into 4G during the cellular architecture.
2. IMSI catchers in 4G
   The main intention of this section is to provide an overview of unfixed vulnerabilities in 4G networks enabling IMSI catchers attacks.
   we explain IMSI catchers attacking techniques in 4G and our previous practical work from Blackhat 2016 on low-cost 4G IMSI catchers.
   At the end of this part, we technically detailed and summarise known vulnerabilities and attacks in 4G networks.
3. 5G networks and RAN security
   Here, we introduce an overview of the 5G security architecture as defined by the 3GPP standards. However, we only focus on 5G RAN ( radio access network) security features protecting privacy aspects. We present detailed security architecture of 5G NSA and SA type - this is important to understand our findings in chapter. We summarise them to give an overview from the complex and over-structured/-jargon standards document. This systematic summary list/tables we use later for the explanations.
4. Identity and IMSI protection features in 5G
   In this section, we discuss the identity and other protection features of 5G subscribers that are introduced to address IMSI catcher threats in 5G.
5. 5G IMSI catchers attack and methods
   In this section, we present issues in the 5G RAN architecture allowing to perform IMSI catchers attack. We present both identify privacy leaking and potential interception possibilities.
   Note that, all of these presented issues are informed to the related 3GPP standard bodies. Some have been

fixed in the current 5G standards and some are not being addressed currently( partly due to complexity/support to legacy systems/difficult to mount targeted attack).

6. Building 5G IMSI catcher
   In this section, we discuss our practical experimental setup of the 5G IMSI catcher. This setup allows us to communicate with currently available 5G mobile devices in the market. We also present our failure and successful attempts with 5G related tools.
7. Experiments with 5G commercial devices
   The goal of this experiment is to demonstrate the feasibility of attacks mentioned in chapter 5 and the efforts required for a modern attacker. We have tested few mobile vendors.
   However, note that the vulnerabilities we presented in chapter 5 are in the 5G standards and affect every 5G mobile phone.
8. Methods to identify 5G subscribers
   In this section, we perform demos to demonstrate the issues presented in chapter 5.
   Live demos from our faraday cage as we guess this will be online talk and not in Vegas. We can run a real 5G network this time in Blackhat LEGALLY ;) and virtually.
9. Intercepting subscriber traffic - legitimate and illegitimate methods
   In this section, we discuss potential ways to intercept 5G subscribers over RAN. Note that we do not cover interception from the 5G core network.
10. Protection techniques and guidelines
    Here, we demonstrate variation in the different 5G mobile vendors and introduced ambiguity for the subscribers.
    Then we explain potential measures that can minimize the impact of the 5G IMSI catchers attack. These measures and guidelines will include mobile vendors, operators, and end-users (subscribers).
11. Conclusion and way forwards to 6G
    We conclude with summary of our findings and directions towards addressing the IMSI catcher problem in 6G networks.

*Notes:*

- *Clearly conveys progression of talk.*
- *Helps the Review Board visualize the presentation in its entirety.*
- *Gives an explanation of each area of the presentation.*

**Attendee Takeaways (What are three actionable takeaways included in your presentation?)**

1. Attendees will learn new protection mechanisms in 5G and their limitations due to the architecture
2. Attendees will learn in what extend their privacy is protected while using 5G phones and what kind of attacks are still possible
3. Attendees will be able to understand 5G RAN security and enabling them to find suitable solutions to protect their related business verticals or digital life which recorded by the phones 24/7.

*Notes:*

- *Submitter fulfilled requirement of providing 3 takeaways*
- *Explains relevance to the audience*
- *Cleary emphasizes the participant benefits*